MULTI-VALUED CROSS-CORRELATION FUNCTIONS BETWEEN TWO MAXIMAL LINEAR RECURSIVE SEQUENCES

Yoji Niho

University of Southern California

Prepared for:

Army Research Office

January 197?

UNCLASSIFIED

Security Classification

AD 786066

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1 ORIGINATING ACTIVITY (Corporate author)

Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

2a. REPORT SECURITY CLASSIFICATION

UNCLASSIFIED

2b. GROUP

3 REPORT TITLE

MULTI-VALUED CROSS-CORRELATION FUNCTIONS BETWEEN TWO MAXIMAL LINEAR RECURSIVE SEQUENCES

4 DESCRIPTIVE NOTES (Type of report and inclusive dates)

Scientific Interim

5 AUTHOR(S) (First name, middle initial, last name)

Yoji Niho

6 REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
January 1972	115	22

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
DA ARO-D-31-124-70-G104 DA ARO-D-31-124-70-G930	USCEE Report 409
b. PROJECT NO 7193-RT, 7198-RT	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
c.	
d.	

10 DISTRIBUTION STATEMENT

This document has been approved for public release and sale; its distribution is unlimited.

11 SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	The U.S. Army Research Office-Durham, Durham, North Carolina.

13 ABSTRACT

The cross-correlation function, $\Delta_r(y)$, between two maximal linear recursive sequences is defined by

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)}$$

for some r, $GCD(r, 2^n-1) = 1$. $\Delta_r(y)$ is analyzed and evaluated for two types of decimation r. For the first type, $r \equiv 2^k \bmod 2^{n/2}-1$. It is shown that $\Delta_r(y)$ is restricted to the form

$$\Delta_r(y) = 2^{n/2}(j-1), \quad 0 \leq j \leq J,$$

where j is the number of distinct solutions to the system of two equa-

DD FORM 1 NOV 68 1473

UNCLASSIFIED

Security Classification

tions over $GF(2^n)$ and J is the degree of one of the two equations. For the second type, $r = (2^{mk}+1)/(2^k+1)$ and for this case $\Delta_r(y)$ is restricted to the form

$$\Delta_r(y) = 0, \quad \pm 2^{(n+de)/2}, \quad 0 \leq d \leq m-2, \quad d \text{ odd}$$

where $e = GCD(n,k)$ and d depends on the rank of a quadratic form over $GF(2^e)$.

The explicit evaluation of $\Delta_r(y)$ is equivalent to the explicit evaluation of weight distribution of the $(2^n-1,2n)$ cyclic code whose dual code is generated by $f_1(x)f_r(x)$, the product of two primitive polynomials of degree n.

USCEE Report 409

MULTI-VALUED CROSS-CORRELATION FUNCTIONS BETWEEN TWO MAXIMAL LINEAR RECURSIVE SEQUENCES

Yoji Niho

January 1972

Department of Electrical Engineering
University of Southern California
Los Angeles, California 90007

A dissertation presented to the Graduate School, University of Southern California in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Electrical Engineering).

This work was supported in part by the U.S. Army Research Office-Durham under Grant DA-ARO-D-31-124-70-G930 (G1044, G51, G104).

ACKNOWLEDGEMENTS

The author wishes to express his most profound gratitude and appreciation to Dr. Lloyd R. Welch, the Chairman of his Dissertation Committee, for his continual guidance, assistance and encouragement. Numerous ideas on evaluation of cross-correlation functions were suggested by Dr. Welch. The author also wishes to express his gratitude and appreciation to Dr. Solomon W. Golomb and Dr. Albert L. Whiteman who have served on the Dissertation Committee.

ABSTRACT

The cross-correlation function, $\Delta_r(y)$, between two maximal linear recursive sequences is defined by

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)}$$

for some r, $GCD(r,2^n-1) = 1$. $\Delta_r(y)$ is analyzed and evaluated for two types of decimation r. For the first type, $r \equiv 2^k \bmod 2^{n/2}-1$. It is shown that $\Delta_r(y)$ is restricted to the form

$$\Delta_r(y) = 2^{n/2}(j-1), \quad 0 \leq j \leq J,$$

where j is the number of distinct solutions to the system of two equations over $GF(2^n)$ and J is the degree of one of the two equations. For the second type, $r = (2^{mk}+1)/(2^k+1)$ and for this case $\Delta_r(y)$ is restricted to the form

$$\Delta_r(y) = 0, \ \pm 2^{(n+de)/2}, \quad 0 \leq d \leq m-2, \quad d \text{ odd}$$

where $e = GCD(n,k)$ and d depends on the rank of a quadratic form over $GF(2^e)$.

The explicit evaluation of $\Delta_r(y)$ is equivalent to the explicit evaluation of weight distribution of the $(2^n-1,2n)$ cyclic code whose dual code is generated by $f_1(x)f_r(x)$, the product of two primitive polynomials of degree n.

TABLE OF CONTENTS

MULTI-VALUED CROSS-CORRELATION FUNCTIONS BETWEEN TWO MAXIMAL LINEAR RECURSIVE SEQUENCES

CHAPTER I

INTRODUCTION

1. INTRODUCTION

In recent years, maximal linear recursive sequences have been studied extensively, notably by Zierler [1], Gold [2] [3] [4] [5], Kasami [6] [7] [8], Solomon [9], Golomb [10] [11], Welch [12] and Trachtenberg. [13] Maximal linear recursive sequences have ideal auto-correlation values: $C_{aa}(\tau) = -1$ for all $\tau \neq 0$ and $C_{aa}(0)$ = period of the sequence. This ideal auto-correlation property is useful in synchronization technique in communication systems. Some maximal linear recursive sequences have uniformly low cross-correlation values which is responsible for extensive application in spread spectrum communication systems for multiplexing operations. [4]

What is involved in study of the cross-correlation functions between two maximal linear recursive sequences is to evaluate explicitly a quantity $\Delta_r(y)$ where

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)}.$$

Generally it is difficult to evaluate $\Delta_r(y)$ algebraically. However, when the decimation r takes on some special values, the explicit evaluation of $\Delta_r(y)$ is possible. Gold, Kasami and Solomon evaluated $\Delta_r(y)$ for the case $r = 2^k + 1$, $n/GCD(n,k)$ odd. Kasami and Solomon found

the weight distribution formula of the $(2^n-1,2n)$ cyclic code generated by the polynomial $f_1(x)f_r(x)$ via linear recursion. The evaluation of weights of the above cyclic code is equivalent to the evaluation of $\Delta_r(y)$. Welch evaluated $\Delta_r(y)$ for the case $r = 2^{2k} - 2^k + 1$, $n/GCD(n,k)$ odd. Trachtenberg extended the above two results to non-binary cases. He introduced a quantity

$$\Delta'_r(y) = \sum_{x \in GF(p^n)} \rho^{Tr(xy - x^r)}$$

where p is an odd prime and ρ is a complex p-th root of unity. He evaluated $\Delta'_r(y)$ for the cases $r = (p^{2k} + 1)/2$ and $r = (p^{2k} - p^k + 1)$, n odd, $r \not\equiv p^j \mod p^n-1$ for any j. In this paper only the binary cases are considered.

In CHAPTER I fundamental concepts of linear recursive sequences are introduced. All materials are discussed extensively in [10] and [14]. Also given are known results on 3-valued $\Delta_r(y)$ and a relationship between weights of the $(2^n-1,2n)$ cyclic code and cross-correlation values.

In CHAPTER II some properties are presented on $\Delta_r(y)$ including $\Delta_{-1}(y)$. Also presented are useful lemmas on greatest common divisors of two integers and the complete results on 3-valued, 4-valued and 5-valued $\Delta_r(y)$.

In CHAPTER III $\Delta_r(y)$ for the case $r \equiv 2^k \mod 2^{n/2}-1$, $GCD(r,2^n-1) = 1$, is considered.

In CHAPTER IV $\Delta_r(y)$ for the case $r = (2^{mk}+1)/(2^k+1)$, $n/GCD(n,k)$ and m odd, is considered. Also given are some

conjectures on 3-valued and 5-valued $\Delta_r(y)$.

In CHAPTER V summary and comments are given.

2. LINEAR RECURSIVE SEQUENCES

A linear recursive sequence $a_0, a_1, a_2, \ldots$ is a sequence $\{a_i\}$ which satisfies a recursion relation of the form:

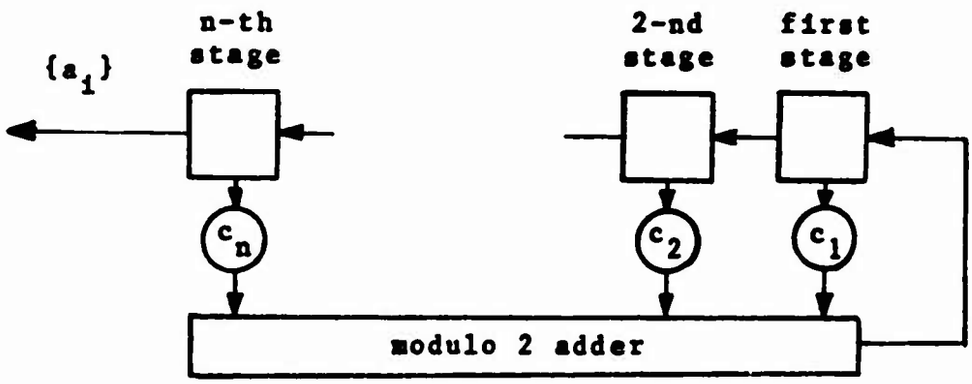
$$a_{n+i} = \sum_{j=1}^{n} c_j a_{n+i-j} \qquad i = 0, 1, 2, \ldots \qquad (1.1)$$

where

$$a_i, c_i \in GF(2)$$

and $a_0, a_1, \ldots, a_{n-1}$ are pre-assigned.

Such a sequence $\{a_i\}$ can be generated by the n-stage shift register and a modulo 2 adder as shown below.



Constants $c_1, c_2, \ldots, c_n$ are feedback coefficients; $c_i = 1$ if there is a tap connected to the i-th stage and $c_i = 0$ if there is no tap connected to the i-th stage. The linear recursive sequence $\{a_i\}$ of (1.1) can be thought as the sequence of outputs observed from the n-th stage.

Initial conditions $a_0, a_1, \ldots, a_{n-1}$ are pre-assigned with the k-th stage containing a_{n-k}, $1 \leq k \leq n$. Contents of stages are added modulo 2 according to the recursion relation (1.1) and the sum is fed back to the first stage as the content of the i-th stage is shifted into the (i+1)-st stage, $1 \leq i \leq n-1$, and the output a_j is shifted out from the n-th stage.

It is said that the sequence $\{a_i\}$ is generated by the polynomial f(x) via linear recursion where

$$f(x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \ldots + c_n. \qquad (1.2)$$

In this paper only sequences considered are those whose recursion polynomial f(x) is irreducible.

In order to describe the sequence $\{a_i\}$ mathematically, consider the sequence $\{b_j\}$ defined by $b_j = a_{n+j}$. Then, the sequence $\{b_j\}$ can be characterized by its Z-transform in terms of the recursion polynomial f(x) of the sequence $\{a_i\}$ and initial conditions $a_0, a_1, \ldots, a_{n-1}$. Let B(z) be the Z-transform of the sequence $\{b_j\}$:

$$B(z) = b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \ldots .$$

Then, B(z) can be expressed as follows:

$$B(z) = \frac{\sum_{j=1}^{n} c_j z^j \{ \sum_{i=0}^{j-1} a_{n-j+i} z^{i-j} \}}{z^n f(1/z)} \qquad (1.3)$$

Many interesting properties of the sequence $\{b_j\}$ can be derived by investigating B(z).[10] However, it is necessary to expand (1.3) if one is to determine $\{b_j\}$.

The period p of the sequence $\{a_i\}$ is the smallest positive integer p such that $a_{i+p} = a_i$ for all i. In terms of the recursion polynomial f(x), the period p is the smallest positive integer p such that f(x) divides $(x^p + 1)$. When $p = 2^n-1$, the polynomial f(x) is said to be primitive. Since f(x) is irreducible, the period p of the sequence $\{a_i\}$ is some divisor of (2^n-1). When $p = 2^n-1$, the sequence $\{a_i\}$ is said to be a maximal linear recursive sequence or a maximal-length linear shift register sequence. The sequence $\{a_i\}$ is a maximal linear recursive sequence if and only if its recursion polynomial f(x) is primitive. For the remainder of this paper, only the maximal linear recursive sequence $\{a_i\}$ is considered and the analysis is made on $\{a_i\}_{i=0}^{2^n-2}$. A maximal linear recursive sequence is henceforth simply referred to as a maximal sequence.

A more algebraic representation of a maximal sequence $\{a_i\}_{i=0}^{2^n-2}$ generated by (1.1), which gives more insight to the structure of such a sequence, is the following: [14]

$$a_i = Tr_1^n(\beta\alpha^i) \tag{1.4}$$

where

α is the root of f(x) of (1.2),

$Tr_e^n(x)$ is the trace linear functional Tr_e^n on $GF(2^n)$ defined by

$$Tr_e^n(x) = x + x^{2^e} + x^{2^{2e}} + \ldots + x^{2^{(n-1)e}} \tag{1.5}$$

and β is some element of $GF(2^n)$.

The element β is determined uniquely by initial conditions $a_0, a_1, \ldots, a_{n-1}$ from the following matrix-vector equation:

$$\underline{D}\,\underline{x}^t = \underline{y}^t$$

where

$$\underline{D} = (d_{i,j}),\ 1 \le i,j \le n,$$

$$\underline{x} = (x_i),\ \underline{y} = (y_i),\ 1 \le i \le n,$$

$$d_{i,j} = \alpha^{(i-1)2^{j-1}},$$

$$x_i = \beta^{2^{i-1}},$$

$$y_i = a_{i-1},$$

a_i, α and β are as defined above

and t indicates the transpose.

Since the determinant $|D|$ is a van der Monde determinant, a vector $\underline{x}$ and hence β can be determined uniquely from $\underline{y}$.

Since for any $x, y \in GF(2^n)$ and for all i, $(x + y)^{2^i} = x^{2^i} + y^{2^i}$ and $x^{2^n} = x$, the following important properties of $Tr_e^n(x)$ are true:

$$Tr_e^n(x) \in GF(2^e)$$

$$Tr_e^n(x + y) = Tr_e^n(x) + Tr_e^n(y)$$

$$Tr_e^n(x^{2^i}) = Tr_e^n(x)$$

A maximal sequence $\{a_i\}_{i=0}^{2^n-2}$ is said to be in natural orientation if $a_i = a_{2i}$ for all i, indices reduced modulo 2^n-1. Such a sequence does exist and it is obtained when initial conditions $a_0, a_1, \ldots, a_{n-1}$ are given by:

$$a_i = Tr_1^n(\alpha^i) \tag{1.6}$$

That is, $\beta = 1$ in (1.4). Henceforth, when we consider a maximal sequence $\{a_i\}_{i=0}^{2^n-2}$ in natural orientation, it is understood that a_i is given by (1.6) for all i.

Throughout this paper a symbol "n" is reserved to represent the degree of the recursion polynomial f(x) in (1.2) or equivalently the number of stages used to generate a sequence $\{a_i\}$. A notation Tr is often used in place of Tr_1^n. When a confusion can arise, Tr_1^n will be used explicitly.

Given two integers r and q, GCD(r,q) is the greatest positive integer that divides both r and q, and LCM(r,q) is the least positive integer that is divisible by both r and q. Given two polynomials s(x) and t(x), GCD(s(x),t(x)) is the monic polynomial of greatest degree that divides both s(x) and t(x).

A sequence $\{b_i\}$ is said to be obtained by decimation r from a sequence $\{a_i\}$ when $b_i = a_{ri}$, indices reduced modulo 2^n-1. Let $\{b_i\}$ be the sequence obtained from $\{a_i\}$ by decimation r. When $\{a_i\}$ is maximal, $\{b_i\}$ is also maximal provided that $GCD(r,2^n-1) = 1$. If $\{a_i\}$ is in natural orientation and $GCD(r,2^n-1) = 1$, then $\{b_i\}$ is also in natural orientation. If f(x) is a recursion polynomial for $\{a_i\}$, then h(x) is a recursion polynomial for $\{b_i\}$ provided that h(x) is the minimal polynomial of α^r and α is the root of f(x).

There are $\phi(p)$ integers from 1 to p which are relatively prime to p, where $\phi(p)$ is the Euler ϕ - function. These $\phi(p)$ integers form a group G under multiplication modulo p. Let $p = 2^n - 1$. Then, the set $H = \{ 1, 2, 2^2, \ldots, 2^{n-1} \}$ forms a multiplicative subgroup of G. Proper cyclotomic cosets, C_i, of H can be obtained by multiplying elements of H by an element of G. That is,

$C_1 = g_1H$, $g_1 = 1$

$C_2 = g_2H$, $g_2 \in G$ but $g_2 \notin C_1$

.....

$C_i = g_iH$, $g_i \in G$ but $g_i \notin C_j$ for all j, $1 \leq j < i$

.....

There are exactly $\phi(2^n-1)/n$ proper cyclotomic cosets. A cyclotomic coset $C = rH$ is called improper if $GCD(r,2^n-1) \neq 1$, $1 \leq r \leq 2^n-1$. Proper cyclotomic cosets and improper cyclotomic cosets constitute cyclotomic cosets modulo 2^n-1. There are $\{-1 + \frac{1}{n} \sum_{d|n} \phi(d)2^{n/d}\}$ cyclotomic cosets in all. q and r belong to the same cyclotomic coset if and only if there exists some integer j, $0 \leq j \leq n-1$, such that $q \equiv 2^j r \mod 2^n-1$. The smallest member of the cyclotomic coset is called the cyclotomic coset leader.

Let C_q and C_r be cyclotomic cosets containing q and r respectively. Then, C_q is called the inverse cyclotomic coset of C_r if there exists some integer j, $0 \leq j \leq n-1$, such that $qr \equiv 2^j \mod 2^n-1$.

Two maximal sequences $\{b_i\}$ and $\{b'_i\}$ obtained by

decimations r and r' respectively from the same maximal sequence $\{a_i\}$ in natural orientation are identical if r and r' belong to the same proper cyclotomic coset.

There are $\phi(2^n-1)/n$ distinct maximal sequences of period $2^n - 1$. They are generated by $\phi(2^n-1)/n$ distinct primitive polynomials of degree n. Given one maximal sequence $\{a_i\}$, remaining $\{\phi(2^n-1)/n - 1\}$ maximal sequences can be obtained from $\{a_i\}$ by decimations r_2, r_3, ... , $r_{\phi(2^n-1)/n}$, where r_i is any member of the i-th proper cyclotomic coset C_i.

The following lemma is a well known result of finite fields. It is often used in evaluation of cross-correlation functions between two maximal sequences.

LEMMA 1-1:

$$\sum_{x \in GF(2^n)} (-1)^{Tr(\sigma x)} = \begin{cases} 2^n & \text{if } \sigma = 0 \\ 0 & \text{if } \sigma \neq 0,\ \sigma \in GF(2^n) \end{cases}$$

proof:

If $\sigma = 0$, the result is trivial. If $\sigma \neq 0$, σx is equal to each element of $GF(2^n)$ exactly once as x ranges over $GF(2^n)$. Hence,

$$\sum_{x \in GF(2^n)} (-1)^{Tr(\sigma x)} = \sum_{x \in GF(2^n)} (-1)^{Tr(x)}$$

Since $x \in GF(2^n)$ if and only if $x + x^{2^n} = 0$ and

$$x + x^{2^n} = (x + x^2 + \ldots + x^{2^{n-1}})(1 + x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}})$$

$$= Tr(x)\{1 + Tr(x)\},$$

exactly half of the elements have trace 1 and the others have trace 0. Hence

$$\sum_{x \in GF(2^n)} (-1)^{Tr(x)} = 0 \qquad \text{QED}$$

3. CROSS-CORRELATION FUNCTIONS BETWEEN 2 MAXIMAL SEQUENCES

An auto-correlation function $C_{aa}(\tau)$ of a maximal sequence $\{a_i\}_{i=0}^{2^n-2}$ is defined as the number of bit-by-bit agreements minus the number of bit-by-bit disagreements between $\{a_{i+\tau}\}_{i=0}^{2^n-2}$ and $\{a_i\}_{i=0}^{2^n-2}$, indices reduced modulo 2^n-1. Then, $C_{aa}(\tau)$ can be expressed as

$$C_{aa}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{a_{i+\tau}} (-1)^{a_i}, \quad 0 \leq \tau \leq 2^n-2.$$

The auto-correlation function $C_{aa}(\tau)$ of a maximal sequence is a two-valued function as shown in the following well-known theorem.

THEOREM 1-2: [1] [10]

$$C_{aa}(\tau) = \begin{cases} -1 & \text{for } \tau \neq 0 \\ 2^n-1 & \text{for } \tau = 0 \end{cases}$$

proof:

Using (1.6), $C_{aa}(\tau)$ can be expressed as

$$C_{aa}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{Tr(\alpha^{i+\tau})} (-1)^{Tr(\alpha^i)}$$

$$= \sum_{i=0}^{2^n-2} (-1)^{Tr(\alpha^{i+\tau} + \alpha^i)}.$$

As i ranges from 0 to 2^n-2, α^i takes on all non-zero elements of $GF(2^n)$ once. Then, by letting $\alpha^\tau = y \in GF(2^n)$,

$$C_{aa}(\tau) = \sum_{\substack{x \in GF(2^n) \\ x \neq 0}} (-1)^{Tr(xy + x)}$$

$$= \sum_{\substack{x \in GF(2^n) \\ x \neq 0}} (-1)^{Tr\{x(y+1)\}}$$

$$= -1 + \sum_{x \in GF(2^n)} (-1)^{Tr\{x(y+1)\}}.$$

Using Lemma 1-1,

$$= \begin{cases} -1 & \text{if } y \neq 1 \\ -1+2^n & \text{if } y = 1 \end{cases}$$

$$= \begin{cases} -1 & \text{if } \tau \neq 0 \\ -1+2^n & \text{if } \tau = 0 \end{cases}$$

QED

A cross-correlation function $C_{ab}(\tau)$ between two maximal sequences $\{a_i\}_{i=0}^{2^n-2}$ and $\{b_i\}_{i=0}^{2^n-2}$ is defined similarly.

$$C_{ab}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{a_{i+\tau}} (-1)^{b_i}$$

Let $\{b_i\}_{i=0}^{2^n-2}$ be a maximal sequence obtained from $\{a_i\}_{i=0}^{2^n-2}$ by proper decimation r. That is, $b_i = a_{ri}$ and $GCD(r, 2^n-1) = 1$. Then,

$$C_{ab}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{a_{i+\tau}} (-1)^{a_{ri}}$$

$$= \sum_{i=0}^{2^n-2} (-1)^{Tr(\alpha^{i+\tau} + \alpha^{ri})}$$

$$= \sum_{\substack{x \in GF(2^n) \\ x \neq 0}} (-1)^{Tr(xy + x^r)}$$

where $y = \alpha^r$. Then,

$$C_{ab}(\tau) = -1 + \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)}.$$

The following two theorems are known.

THEOREM 1-3: Gold [5], Kasami [6] [7] [8], Solomon [9]

If $r = 2^k + 1$ and n/e is odd where $e = GCD(n,k)$, $C_{ab}(\tau)$ takes on only three values: -1, $-1 \pm 2^{(n+e)/2}$.

$$C_{ab}(\tau) = \begin{cases} -1+2^{(n+e)/2} & 2^{n-e-1}+2^{(n-e-2)/2} \text{ times} \\ -1 & 2^n - 2^{n-e} - 1 \text{ times} \\ -1-2^{(n+e)/2} & 2^{n-e-1}-2^{(n-e-2)/2} \text{ times} \end{cases} \quad (1.7)$$

THEOREM 1-4: Golomb [11], Welch [12]

If $r = 2^{2k} - 2^k + 1$ and n/e is odd where $e = GCD(n,k)$, $C_{ab}(\tau)$ takes on only three values. The distribution of cross-correlation values are again given by (1.7).

The conjecture [11] that for n odd $r = 2^{(n-1)/2} + 2^d + 1$ where d is a divisor of (n-1) leads to the three-valued $C_{ab}(\tau)$ was shown to be false. Some of the counter-examples are given below.

n	d	r	$C_{ab}(\tau)$
7	6	73	7-valued
11	2	37	5-valued
11	10	$1057 \equiv 67$	9-valued
13	2	69	10-valued

13	3	73	18-valued
13	4	81	9-valued
13	12	$4161 \equiv 131$	19-valued

However, the Welch's conjecture [11] that $r = 2^{(n-1)/2} + 3$ leads to the 3-valued $C_{ab}(\tau)$ has been verified for $n \leq 17$.

Define $\Delta_r(y)$ by

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)}$$

$$= C_{ab}(\tau) + 1$$

where

$$y = \alpha^\tau \text{ and } \{b_i\}_{i=0}^{2^n-2} = \{a_{ri}\}_{i=0}^{2^n-2}.$$

For the remainder of this paper, by the cross-correlation function, we shall mean $\Delta_r(y)$ rather than $C_{ab}(\tau)$.

Let $n(\Delta_r)$ denote the number of times $\Delta_r(y)$ takes on the value Δ_r as y ranges over $GF(2^n)$. In terms of $\Delta_r(y)$ Theorem 1-3 and Theorem 1-4 become:

THEOREM 1-5:

If $r = 2^k + 1$ and n/e is odd where $e = GCD(n,k)$, $\Delta_r(y)$ takes on three values: $0, \pm 2^{(n+e)/2}$

Δ_r	$n(\Delta_r)$	
$2^{(n+e)/2}$	$2^{n-e-1} + 2^{(n-e-2)/2}$	
0	$2^n - 2^{n-e}$	(1.8)
$-2^{(n+e)/2}$	$2^{n-e-1} - 2^{(n-e-2)/2}$	

THEOREM 1-6:

If $r = 2^{2k} - 2^k + 1$ and n/e is odd where $e = GCD(n,k)$, $\Delta_r(y)$ takes on three values. Δ_r and $\eta(\Delta_r)$ are given by (1.8).

For the remainder of this paper, an analysis is made on $\Delta_r(y)$ instead of $C_{ab}(\tau)$.

The complete evaluation of $\Delta_r(y)$ for n = 3 through n = 12 has been carried out on IBM 370 at the University Computing Center. For n = 13 through n =15, only those proper decimations that lead to 7 or less distinct cross-correlation values are determined. For n = 16, only those that lead to 5 or less cross-correlation values are determined. In obtaining these results, the author used the Fourier transform algorithm developed by Welch.

Table 1-1 lists coset leaders of the cyclotomic cosets containing r and r^{-1} where r is given by Theorems 1-5 and 1-6. Table 1-2 lists decimations that result in 3-valued $\Delta_r(y)$ for n = 3 through n = 16 that are not covered by either Theorem 1-5 or Theorem 1-6. Two decimations r and r' are given in pair as the cyclotomic cosets containing r and r' are inverse of each other. The complete results appear in APPENDIX A.

4. $(2^n-1,2n)$ CYCLIC CODES

Theorems on cross-correlation values Δ_r and their

CYCLOTOMIC COSET LEADERS GIVEN BY THEOREMS 1-5 & 1-6

			THEOREM 1-5		THEOREM 1-6	
	k	e	r	r^{-1}	r	r^{-1}
n = 3	1	1	3	3	3	3
n = 5	1	1	3	11	3	11
	2	1	5	7	11	3
n = 6	2	2	5	13	13	5
n = 7	1	1	3	43	3	43
	2	1	5	27	13	11
	3	1	9	15	23	29
n = 9	1	1	3	171	3	171
	2	1	5	103	13	59
	3	3	9	57	57	9
	4	1	17	31	47	87
n = 10	2	2	5	205	13	79
	4	2	17	181	79	13
n = 11	1	1	3	683	3	683
	2	1	5	411	13	315
	3	1	9	231	57	413
	4	1	17	365	143	43
	5	1	33	63	95	151

n = 12	4	4	17	241	241	17
n = 13	1	1	3	2731	3	2731
	2	1	5	1639	13	635
	3	1	9	911	57	723
	4	1	17	1453	241	171
	5	1	33	1243	287	1691
	6	1	65	127	191	1245
n = 14	2	2	5	3277	13	1339
	4	2	17	2893	241	205
	6	2	65	2773	319	979
n = 15	1	1	3	10923	3	10923
	2	1	5	6555	13	2523
	3	3	9	3641	57	575
	4	1	17	1935	241	3671
	5	5	33	993	993	33
	6	3	65	3529	575	57
	7	1	129	255	383	4791

TABLE 1-1

INVERSE PAIRS OF COSET LEADERS GIVING 3-VALUED $\Delta_r(y)$

n = 9	19 - 27	
n = 10	25 - 41	49 - 107
n = 11	35 - 117	107 - 249
n = 13	67 - 367	71 - 347
n = 14	113 - 145	193 - 1613
n = 15	131 - 4815	1371 - 2033

TABLE 1-2

distribution $\eta(\Delta_r)$ as y ranges over $GF(2^n)$ can be translated to theorems on weight w and weight distribution $\eta(w)$ of a $(2^n-1,2n)$ cyclic code.

Let C be the $(2^n-1,2n)$ cyclic code generated by the polynomial $f_1(x)f_r(x)$ via linear recursion. That is, C is the $(2^n-1,2n)$ cyclic code whose generator polynomial [15] is given by:

$$(x^{2^n-1} + 1)/x^{2n} f_1(1/x) f_r(1/x)$$

where

$f_i(x)$ is the minimal polynomial of α^i and α is a primitive element of $GF(2^n)$.

Then, given a codeword $\underline{a} = (a_0, a_1, a_2, \ldots, a_{2^n-2})$ in C, there exist two elements c and d in $GF(2^n)$ such that the Mattson-Solomon polynomial associated with $\underline{a}$ is given by $g_{\underline{a}}(x) = Tr(cx) + Tr(dx^r)$ and $a_i = g_{\underline{a}}(\alpha^i)$. Note that $c = 0 = d$ corresponds to the case $w(\underline{a}) = 0$ and $c = 0$, $d \neq 0$ or $c \neq 0$, $d = 0$ corresponds to the case $w(\underline{a}) = 2^{n-1}$.

The non-zero weight w and the weight distribution $\eta(w)$ of the $(2^n-1,2n)$ cyclic code C are related to Δ_r and $\eta(\Delta_r)$ as follows:

$$\begin{aligned} w &= (2^n - \Delta_r)/2 \\ \eta(w) &= (2^n - 1)\eta(\Delta_r) && \text{for } \Delta_r \neq 0 \\ \eta(w) &= (2^n - 1)\{\eta(\Delta_r) + 1\} && \text{for } \Delta_r = 0 \end{aligned} \qquad (1.9)$$

The minimum weight w_{min} of C is given by:

$$w_{min} = \{2^n - \max_y \Delta_r(y)\}/2.$$

In terms of cyclic codes, Theorem 1-5 and Theorem 1-6 become :

The $(2^n-1,2n)$ cyclic code generated by the polynomial $f_1(x)f_r(x)$ via linear recursion is a tri-weight code with the following weight distribution for non-zero weight.

w	n(w)
$2^{n-1} - 2^{(n+e-2)/2}$	$(2^n - 1)(2^{n-e-1} + 2^{(n-e-2)/2})$
2^{n-1}	$(2^n - 1)(2^n - 2^{n-e} + 1)$
$2^{n-1} + 2^{(n+e-2)/2}$	$(2^n - 1)(2^{n-e-1} - 2^{(n-e-2)/2})$

where

$r = 2^k + 1$ or $r = 2^{2k} - 2^k + 1$,

$e = GCD(n,k)$

and n/e is odd.

CHAPTER II

PROPERTIES OF CROSS-CORRELATION FUNCTIONS

1. FURTHER RESULTS ON $\Delta_r(y)$

In this section, we derive some results on $\Delta_r(y)$. The first three lemmas are the direct results of the structures of finite fields. Proofs are omitted.

LEMMA 2-1:

$\Delta_r(y) = \Delta_r(y^{2^k})$ for all k.

LEMMA 2-2:

If r and r' belong to the same proper cyclotomic coset, $\Delta_r(y) = \Delta_{r'}(y)$ for all y.

LEMMA 2-3:

If two proper decimations r and r' are such that $r \cdot r' \equiv 2^k \mod 2^n-1$, $\Delta_r(y) = \Delta_{r'}(y^{-r})$.

LEMMA 2-4:

$\Delta_r(y) \equiv 0 \mod 4$ for all y and r, $GCD(r,2^n-1) = 1$.

proof:

Let N(i,j) be the number of times the ordered pair {Tr(xy) = i and $Tr(x^r) = j$} occurs as x ranges over $GF(2^n)$.

Both mappings $x \to xy$, $y \neq 0$, and $x \to x^r$, $GCD(r,2^n-1)$

= 1, permute elements of $GF(2^n)$. Since exactly half of the elements have trace 1 and the others have trace 0, the following 4 equalities hold.

$$N(0,0) + N(0,1) = 2^{n-1}$$

$$N(1,0) + N(1,1) = 2^{n-1}$$

$$N(0,0) + N(1,0) = 2^{n-1}$$

$$N(0,1) + N(1,1) = 2^{n-1}$$

which imply

$$N(0,0) = N(1,1)$$

$$N(1,0) = N(0,1)$$

$N(0,0)$ and $N(1,0)$ are both even or both odd.

From the definition of the cross-correlation function,

$$\Delta_r(y) = \{N(0,0) + N(1,1)\} - \{N(1,0) + N(0,1)\}$$

$$= 2\{N(0,0) - N(1,0)\}.$$

Since $N(0,0)$ and $N(1,0)$ are both even or both odd, $\{N(0,0) - N(1,0)\}$ is even. Hence, $\Delta_r(y) \equiv 0 \mod 4$.

Clearly $\Delta_r(y) = 0$ when $y = 0$. QED

In view of Lemma 2-4, $\Delta_r(y)$ exhibits interesting characteristics for $r = 2^{n-1} - 1$. Since $2r \equiv -1 \mod 2^n-1$, $\Delta_r(y)$ for $r = 2^{n-1} - 1$ is a cross-correlation function between a maximal sequence and its reverse sequence. In [16] Dowling and McEliece gave the bound on $\Delta_{-1}(y)$. They applied the result on exponential sums in finite fields given by Carlitz and Uchiyama. [17]

$$\left| \sum_{\substack{x \in GF(p^n) \\ x \neq 0}} \exp\{\frac{2\pi i}{p} \mathrm{Tr}(xy + x^{-1})\} \right| \leq 2 \cdot p^{n/2}$$

where

$$y \in GF(p^n).$$

Letting $p = 2$,

$$\left| \sum_{\substack{x \in GF(2^n) \\ x \neq 0}} (-1)^{\mathrm{Tr}(xy + x^{-1})} \right|$$

$$= |\Delta_{-1}(y) - 1| \leq 2^{(n+2)/2}$$

Hence,

$$-2^{(n+2)/2} + 1 \leq \Delta_{-1}(y) \leq 2^{(n+2)/2} + 1 \qquad (2.1)$$

Since $2^{(n+2)/2} \equiv 0 \mod 4$ for n even, we have

$$-2^{(n+2)/2} + 4 \leq \Delta_{-1}(y) \leq 2^{(n+2)/2}, \text{ n even} \qquad (2.2)$$

Let L_n denote the number of distinct values that $\Delta_{-1}(y)$ takes on as y ranges over $GF(2^n)$.

It has been verified that the bounds on $\Delta_{-1}(y)$ given by (2.1) and (2.2) are extremely tight for $n \leq 18$ as shown in Table 2-1. For n odd, the largest and the smallest values between the bounds of (2.1) which are of the form 4K are attained by $\Delta_{-1}(y)$ for some y. For n even, both the upper and the lower bounds of (2.2) are attained. Furthermore, since $L_n = \{\max\{\Delta_{-1}(y)\} - \min\{\Delta_{-1}(y)\}\}/4 + 1$ for all $n \leq 18$, $\Delta_{-1}(y)$ takes on all values of the form 4K between the bounds of (2.1).

CROSS-CORRELATION VALUES OF REVERSE SEQUENCES

n	$2^{(n+2)/2}$	$\max_y\{\Delta_{-1}(y)\}$	$\min_y\{\Delta_{-1}(y)\}$	L_n
3	5.7	4	-4	3
4	8	8	-4	4
5	11.3	12	-8	6
6	16	16	-12	8
7	22.6	20	-20	11
8	32	32	-28	16
9	45.3	44	-44	23
10	64	64	-60	32
11	90.5	88	-88	45
12	128	128	-124	64
13	181.02	180	-180	91
14	256	256	-252	128
15	362.0	360	-360	181
16	512	512	-508	256
17	724.1	724	-720	362
18	1024	1024	-1020	512

TABLE 2-1

LEMMA 2-5:

$$\sum_{y\in GF(2^n)} \{\Delta_r(y)\} = 2^n$$

$$\sum_{y\in GF(2^n)} \{\Delta_r(y)\}^2 = 2^{2n}$$

proof:

$$\sum_{y\in GF(2^n)} \{\Delta_r(y)\}$$

$$= \sum_{y\in GF(2^n)} \sum_{x\in GF(2^n)} (-1)^{Tr(xy + x^r)}$$

$$= \sum_{x\in GF(2^n)} (-1)^{Tr(x^r)} \sum_{y\in GF(2^n)} (-1)^{Tr(xy)} = 2^n$$

The last step follows from Lemma 1-1 since the second sum is equal to 0 for all $x \neq 0$ and 2^n for $x = 0$.

$$\sum_{y\in GF(2^n)} \{\Delta_r(y)\}^2$$

$$= \sum_{y\in GF(2^n)} \sum_{x\in GF(2^n)} (-1)^{Tr(xy+x^r)} \sum_{z\in GF(2^n)} (-1)^{Tr(zy+z^r)}$$

$$= \sum_{x,z\in GF(2^n)} (-1)^{Tr(x^r + z^r)} \sum_{y\in GF(2^n)} (-1)^{Tr\{(x + z)y\}}$$

Again from Lemma 1-1, the second sum is equal to 2^n if $x + z = 0$ or $x = z$ and the sum is equal to zero if $x + z \neq 0$. Hence,

$$= 2^n \sum_{\substack{x,z\in GF(2^n) \\ x = z}} (-1)^{Tr(x^r + z^r)} = 2^n \sum_{\substack{x,z\in GF(2^n) \\ x = z}} 1$$

$$= 2^{2n}$$ QED

Lemma 2-5 is useful in evaluating the distribution of $\Delta_r(y)$. In order to obtain the higher moment identities, it

is necessary to evaluate the term

$$\sum_{\substack{x_1 \\ x_1 + x_2 + .. + x_k = 0}} \sum_{x_2} \cdots \sum_{x_k} (-1)^{Tr(x_1^r + x_2^r + .. + x_k^r)}$$

However, it is not trivial to evaluate the above sum.

Let C and C' be the $(2^n-1,2n)$ and the $(2^n-1,2^n-2n-1)$ cyclic codes whose generator polynomials are $(x^{2^n-1} + 1)/x^{2n} f_1(1/x) f_r(1/x)$ and $f_1(x) f_r(x)$ respectively. Let a_i and b_i be the number of codewords of weight i in C and C' respectively. Since C' is a subcode of a cyclic Hamming code, $b_1 = 0 = b_2$. Therefore, following power moment identities of Pless [18] must hold.

$$\sum_j j a_j = 2^{2n-1}(2^n-1)$$

$$\sum_j j^2 a_j = 2^{2n-2}(2^n-1)2^n = 2^{3n-2}(2^n-1)$$

These two power moment identities and two identities of Lemma 2-5 become identical with the substitution of j for w and a_j for $\eta(w)$. The two quantities w and $\eta(w)$ are as given in (1.9)

2. GREATEST COMMON DIVISORS

For $\Delta_r(y)$ to be a legitimate cross-correlation function between two maximal sequences, it is necessary and sufficient that $GCD(r,2^n-1) = 1$. Hence, in the analysis of $\Delta_r(y)$ for some r, it must first be shown that $GCD(r,2^n-1) = 1$. However, for the remainder of this paper, when $\Delta_r(y)$

is mentioned and no specific form is assumed for r, it is understood that $GCD(r,2^n-1) = 1$. The following three lemmas are well known results on greatest common divisors.

LEMMA 2-6:

$$GCD(2^m-1,2^n-1) = 2^{GCD(m,n)} - 1$$

LEMMA 2-7:

$GCD(2^m+1,2^n-1) = 1$ if and only if $n/GCD(m,n)$ is odd.

LEMMA 2-8:

If m and $n/GCD(n,k)$ are both odd, $GCD(\frac{2^{mk}+1}{2^k+1},2^n-1) = 1$.

Lemma 2-7 was assumed in Theorems 1-3 and 1-5. Lemma 2-8 with m = 3 was assumed in Theorems 1-4 and 1-6 since $(2^{3k}+1)/(2^k+1) = 2^{2k} - 2^k + 1$. Using Lemmas 2-6 and 2-7, it is easy to show that the following decimations are all proper. That is, $GCD(r_i,2^n-1) = 1$.

$$r_1 = 2^{n/2+1} - 1 \qquad n \equiv 0 \mod 4 \qquad (2.3)$$

$$r_2 = (2^{n/4}-1)(2^{n/2}+1) + 2 \qquad n \equiv 0 \mod 4 \qquad (2.4)$$

$$r_3 = 2^{n/2} + 3 \qquad n \equiv 0 \mod 2 \qquad (2.5)$$

$$r_4 = 2^{n/2} + 2^{n/2-1} - 1 \qquad n \equiv 2 \mod 4 \qquad (2.6)$$

$$r_5 = 2^{n/2+2} - 3 \qquad n \equiv 0 \mod 2 \qquad (2.7)$$

$$r_6 = 2^{n/2+2} + 2^{n/2} - 3 \qquad n \equiv 0 \mod 2 \qquad (2.8)$$

In CHAPTER III $\Delta_{r_i}(y)$ for these 6 decimations are analyzed.

In CHAPTER IV decimations of the form $(2^{mk}+1)/(2^k+1)$ for m and n/GCD(n,k) odd are considered. However, due to Lemma 2-3, some results can be obtained on 3-valued $\Delta_r(y)$ for decimations of this type. For m = n odd, $\Delta_r(y)$ is a 3-valued function as given in the following lemma.

LEMMA 2-9:

For n odd and $r = (2^{nk}+1)/(2^k+1)$, $\Delta_r(y)$ takes on 3 values. Both Δ_r and $\eta(\Delta_r)$ are given by (1.8).

proof:

From Lemma 2-8, $GCD(r,2^n-1) = 1$. Let $r' = 2^k + 1$. From Lemma 2-7, $GCD(r',2^n-1) = 1$. $rr' = 2^{nk} + 1 \equiv 2 \bmod 2^n-1$. The result follows immediately from Theorem 1-5 and Lemma 2-3. QED

In order to find the multiplicative inverse of $r = 2^{2k} - 2^k + 1 = (2^{3k}+1)/(2^k+1)$ modulo 2^n-1 when GCD(n,3) = 1, consider the following.

Let m' be the multiplicative inverse of 3 mod n. m' exists if and only if GCD(n,3) = 1. m' is odd if n is even. If n is odd, m' can be even or odd.

Define m so that

$$\begin{aligned} m &= m' \text{ when } m' \text{ is odd and} \\ m &= n - m' \text{ when } m' \text{ is even.} \end{aligned} \qquad (2.9)$$

Note that m is always odd.

Now consider $r' = (2^{3km}+1)/(2^{3k}+1)$ where m is given

by (2.9). Then,

$$r \cdot r' = \frac{2^{3k}+1}{2^k+1} \frac{2^{3km}+1}{2^{3k}+1} = \frac{2^{3km}+1}{2^k+1}.$$

When m' is odd, $3m = 3m' = 1 + qn$ for some q.

$$r \cdot r' = \frac{2^{k+qnk}+1}{2^k+1} = \frac{2^k(2^n)^{qk}+1}{2^k+1} \equiv 1 \mod 2^n-1$$

When m' is even, $3m = 3(n-m') = 3n - (1+qn) = -1 + (3-q)n$ for some q.

$$r \cdot r' = \frac{2^{-k+(3-q)nk}+1}{2^k+1} = \frac{2^{-k}(2^n)^{(3-q)k}+1}{2^k+1}$$

$$\equiv \frac{2^{-k}+1}{2^k+1} \mod 2^n-1$$

$$\equiv 2^{n-k} \mod 2^n-1$$

Let $3k \equiv j \mod n$ and define t so that

$$t = n-j \quad \text{when } j > (n-1)/2 \text{ and}$$
$$t = j \quad \text{when } j \leq (n-1)/2 \qquad (2.10)$$

For this choice of t, $r' = (2^{3km}+1)/(2^{3k}+1)$ and $r'' = (2^{mt}+1)/(2^t+1)$ belong to the same cyclotomic coset modulo 2^n-1 and $r \cdot r'' \equiv 2^i \mod 2^n-1$ for some i. Since GCD(n,3) = 1, GCD(n,k) = GCD(n,3k) = GCD(n,t). Hence, the following lemma follows directly from Theorem 1-6 and Lemma 2-3.

LEMMA 2-10:

Suppose GCD(3,n) = 1, GCD(t,n) = e and n/e is odd. Let $r'' = (2^{mt}+1)/(2^t+1)$. Then, $\Delta_{r''}(y)$ takes on 3 values. $\Delta_{r''}$ and $\eta(\Delta_{r''})$ are given by (1.8),

where

$$m = \begin{cases} m' & \text{when } m' \text{ is odd} \\ n - m' & \text{when } m' \text{ is even} \end{cases}$$

m' is the multiplicative inverse of 3 mod n.

3. COMPUTED RESULTS FOR 3-, 4- and 5-VALUED $\Delta_r(y)$

Before proceeding to CHAPTER III, we give the complete results on proper cyclotomic coset leaders r that lead to 3-valued, 4-valued and 5-valued cross-correlation functions $\Delta_r(y)$ for $n \leq 16$. They are listed in Tables 2-2, 2-3 and 2-4 respectively. Two coset leaders r and q are given in pair if $rq \equiv 2^i \bmod 2^n-1$ for some i, $0 \leq i \leq n-1$. If $r^2 \equiv 2^i \bmod 2^n-1$ for some i, $0 \leq i \leq n-1$, the coset leader r is given by itself. The letters following coset leaders give theorems, lemmas and conjectures that explain the corresponding $\Delta_r(y)$. The following notations are used:

A - Theorem 1-5	B - Theorem 1-6
C - Theorem 2-9	D - Theorem 2-10
E - Conj. 4-5 (1)	F - Conj. 4-5 (2) or (3)
G - Conj. 4-5 (4)	H - Conj. 4-5 (5)
J - Theorem 3-6	K - Theorem 3-7
L - Theorem 3-5	M - Theorem 3-8
N - Conj. 4-6 (5)	Ø - Lemma 4-1
P - Conj. 4-3	Q - Conj. 4-4
R - Conj. 4-6 (1)	S - Conj. 4-6 (2)
T - Conj. 4-6 (3)	U - Conj. 4-6 (4)

3-VALUED $\Delta_r(y)$

n = 3 3ABCDEF

n = 5 3ABD- 11BCD 5AF- 7CE

n = 6 5A - 13BGH

n = 7 3AB- 43CD 5A - 27C 9A - 15C
11DE- 13B 23B - 29DF

n = 9 3AB- 171C 5A - 103C 9A - 57BC
13B - 59 17A - 31C 19EF- 27
47B - 87

n = 10 5A - 205 13BD- 79BD 17A - 181
25 - 41H 49G - 107

n = 11 3AB- 683CD 5A - 411C 9A - 231C
13B - 315D 17A - 365C 33A - 63C
35E - 117 43D - 143B 57B - 413D
95B - 151D 107 - 249F

n = 12 17A - 241B

n = 13 3AB- 2731CD 5A - 1639C 9A - 911C
13B - 635D 17A - 1453C 33A - 1243C
57B - 723D 65A - 127C 67E - 367
71F - 347 171D - 241B 191B - 1245D
287B - 1691D

n = 14	5A - 3277	13B - 1339D	17A - 2893
	65A - 2773	113 - 145H	193G - 1613
	205D - 241B	319B - 979D	
n = 15	3AB-10923C	5A - 6555C	9A - 3641C
	13B - 2523	17A - 1935C	33A - 993BC
	57B - 575B	65A - 3529C	129A - 255C
	131E - 4815	241B - 3671	383B - 4791
	1371 - 2033F		

TABLE 2-2

4-VALUED $\Delta_r(y)$

n = 4	7JK		
n = 8	31J - 91L	53K	
n = 12	127J -1387L	457K	
n = 16	511J -21931L	3857K	7399L - 9947L
	11093L -13133L		

TABLE 2-3

5-VALUED $\Delta_r(y)$

n = 6	11M - 23L			
n = 8	19M - 47L	23L - 61N		
n = 9	11ØPS - 93P	23R - 25RT	43P - 107ØP	
	109ØP			
n = 10	35M - 95L	101L - 157L		
n = 11	11ØQ- 189Q	25 - 87	37 - 83	
	47R - 49R	81 - 139	121ØQ- 423Q	
	141 - 363	171Q - 205ØQ	187 - 427	
	221ØQ- 343Q	229 - 295	235ØQ- 429Q	
	311			
n = 12	67M - 191L	73 - 731	253N - 599L	
n = 13	11ØQ- 745ØQ	19S - 485	43Q - 381Q	
	95R - 97R	113T - 363	147 - 949	
	161 - 973	205ØQ- 919ØQ	225 - 405	
	445ØQ- 497ØQ	483Q - 1645Q	631 - 1707	
	683Q - 1643Q	749Q - 1367Q	869Q - 1461Q	
	939Q - 953Q			
n = 14	131M - 383L			
n = 15	11ØP- 2979	43P - 765P	113U - 1451	
	171P - 5557	191R - 193R	205ØP- 4965	
	683P - 5805P	893ØP- 3229	995 - 1943ØP	

	1119 - 3543	1275P - 6605P	1913P - 2895P
	2295P - 3755	2521 - 6827	2731P - 3277P
	2981 - 5463	3643 - 6557P	5783P - 6567P
	5813P		
n = 16	259M - 767L	383L -13261L	1021N - 9949L

TABLE 2-4

CHAPTER III

MULTI-VALUED CROSS-CORRELATION FUNCTIONS I

1. PRELIMINARY

As mentioned in CHAPTER I, generally it is difficult to evaluate $\Delta_r(y)$ algebraically. The case $r = 2^k + 1$, $n/GCD(n,k)$ odd, has been solved by Gold, Kasami and Solomon. The case $r = 2^{2k} - 2^k + 1$, $n/GCD(n,k)$ odd, has been solved by Welch. In this chapter we consider the case:

$$n = 2m \text{ and } r \equiv 2^k \mod 2^m-1.$$

It can be shown that $\Delta_r(y)$ is restricted to the form:

$$\Delta_r(y) = 2^m(j-1),\ 0 \leq j \leq J \text{ for some } J.$$

j is the number of distinct solutions to two equations over $GF(2^n)$. Hence, the upper bound J for $\Delta_r(y)$ can be determined immediately by finding the degrees of equations. In general, however, equations are of high degree and the explicit evaluation of $\Delta_r(y)$ is not trivial.

As mentioned in CHAPTER II, the following six decimations are analyzed in Section 2 of this chapter.

$$r_1 = 2^{n/2+1} - 1 \qquad n \equiv 0 \mod 4 \qquad (3.1)$$

$$r_2 = (2^{n/4}-1)(2^{n/2}+1) + 2 \qquad n \equiv 0 \mod 4 \qquad (3.2)$$

$$r_3 = 2^{n/2} + 3 \qquad n \equiv 0 \mod 2 \qquad (3.3)$$

$$r_4 = 2^{n/2} + 2^{n/2-1} - 1 \qquad n \equiv 2 \mod 4 \qquad (3.4)$$

$$r_5 = 2^{n/2+2} - 3 \qquad n \equiv 0 \mod 2 \qquad (3.5)$$

$$r_6 = 2^{n/2+2} + 2^{n/2} - 3 \qquad n \equiv 0 \mod 2 \qquad (3.6)$$

They are analyzed in Theorems 3-6, 3-7, ... , 3-11 respectively.

In Section 3 computed results are listed. Before the main theorem of this chapter, Theorem 3-5, is introduced, we consider the two preliminary lemmas and two results in solving equations over $GF(2^n)$.

LEMMA 3-1:

When $n = 2m$, non-zero element x of $GF(2^n)$ can be represented as $x = \alpha\beta$, where $\alpha \in GF(2^m)$, $\alpha \neq 0$, and β is (2^m+1)-st root of unity in $GF(2^{2m})$.

proof:

Let $x \in GF(2^{2m})$, $x \neq 0$.

$$2^{2m} = 2^{m-1}(2^m + 1) + 2^{m-1}(2^m - 1)$$

$$x = x^{2^{2m}} = x^{2^{m-1}(2^m+1)} \cdot x^{2^{m-1}(2^m-1)}$$

Letting $\alpha = x^{2^{m-1}(2^m+1)}$ and $\beta = x^{2^{m-1}(2^m-1)}$, it is easy to see that $\alpha^{2^m-1} = 1$ and hence $\alpha \in GF(2^m)$ and that $\beta^{2^m+1} = 1$.

To show the uniqueness of the representation, let ω be a primitive element of $GF(2^{2m})$. Then, elements α and β can be expressed as

$$\alpha = \omega^{(2^m+1)i}, \quad i = 1, 2, \ldots, 2^m-1$$

and $$\beta = \omega^{(2^m-1)j}, \quad j = 1, 2, \ldots, 2^m+1.$$

Assume that there exist elements α, β, α' and β' such that $\alpha\beta = x = \alpha'\beta'$. This says that given some i and j,

there exist $(2^m+1)s = \alpha'$ and $(2^m-1)t = \beta'$ such that

$$\omega^{(2^m+1)i}\,\omega^{(2^m-1)j} = \omega^{(2^m+1)s}\,\omega^{(2^m-1)t},$$

which implies

$$(2^m+1)i + (2^m-1)j \equiv (2^m+1)s + (2^m-1)t \mod 2^{2m}-1.$$

$$(2^m+1)(i-s) \equiv (2^m-1)(t-j) \mod 2^{2m}-1 \qquad (3.7)$$

Let $i \geq s$ without loss of generality. Note that $0 \leq (i-s) \leq 2^m-2$ and $|t-j| \leq 2^m$. From (3.7) we have

$$(2^m+1)(i-s) = (2^m-1)(t-j) + k(2^{2m}-1)$$

$$= (2^m-1)\{k(2^m+1) + (t-j)\} \qquad (3.8)$$

for some k, k = 0 or k = 1. (3.8) implies that

$$\mathrm{LCM}(2^m+1, 2^m-1) \leq (2^m+1)(2^m-2) = 2^{2m} - 2^m - 2.$$

But since $\mathrm{GCD}(2^m+1, 2^m-1) = 1$, we must have

$$\mathrm{LCM}(2^m+1, 2^m-1) = (2^m+1)(2^m-1) = 2^{2m} - 1.$$

This is a contradiction. The only way in which (3.8) holds without contradiction is i = s, t = j and k = 0. Or $\alpha = \alpha'$ and $\beta = \beta'$. QED

LEMMA 3-2:

Let n = 2m, $\alpha \in GF(2^m)$ and $\beta \in GF(2^{2m})$. Then

$$\mathrm{Tr}_1^{2m}(\alpha\beta) = \mathrm{Tr}_1^m\{\alpha(\beta + \beta^{2^m})\}.$$

proof:

$$\mathrm{Tr}_1^{2m}(\alpha\beta) = \sum_{j=0}^{2m-1} (\alpha\beta)^{2^j}$$

$$= \sum_{j=0}^{m-1} (\alpha\beta)^{2^j} + \sum_{j=m}^{2m-1} (\alpha\beta)^{2^j}$$

$$= \sum_{j=0}^{m-1} (\alpha\beta)^{2^j} + \sum_{j=0}^{m-1} (\alpha\beta)^{2^j 2^m}$$

$$= \sum_{j=0}^{m-1} (\alpha\beta)^{2^j} + \sum_{j=0}^{m-1} (\alpha\beta^{2^m})^{2^j}$$

$$= \sum_{j=0}^{m-1} \{\alpha(\beta + \beta^{2^m})\}^{2^j}$$

$$= Tr_1^m\{\alpha(\beta + \beta^{2^m})\} \qquad \text{QED}$$

In order to derive an explicit formula for $\Delta_r(y)$, it becomes necessary to find the number of distinct solutions to the equations over $GF(2^n)$. Following two lemmas are useful in finding the number of solutions.

LEMMA 3-3: McEliece [19]

The equation $x^{2^k} + x = y$, $y \in GF(2^n)$, $k < n$, has either no roots or 2^e roots in $GF(2^n)$. It has 2^e roots if and only if $Tr_e^n(y) = 0$, where $e = GCD(n,k)$.

LEMMA 3-4:

A polynomial $g(x)$ is a repeated factor of a polynomial $f(x)$ if and only if $g(x)$ divides $GCD(f(x),f'(x))$, where $f'(x)$ is the formal derivative of $f(x)$.

2. $\Delta_r(y)$ FOR $r \equiv 2^k \mod 2^{n/2}-1$

The crux for analyzing this type of $\Delta_r(y)$ is the following theorem, which was suggested by Welch.

THEOREM 3-5:

If $n = 2m$, $GCD(r, 2^n-1) = 1$ and $r \equiv 2^k \mod 2^m-1$ for some k, $0 \leq k \leq m-1$, then $\Delta_r(y) = 2^m(j-1)$, $0 \leq j \leq J$, for some j and J.

proof:

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)}$$

$$= 1 + \sum_{\substack{x \in GF(2^n) \\ x \neq 0}} (-1)^{Tr(xy + x^r)}$$

Using Lemma 3-1, let $x = \alpha\beta$ where $\alpha \in GF(2^m)$, $\alpha \neq 0$, and $\beta^{2^m+1} = 1$, $\beta \in GF(2^{2m})$. Then,

$$\Delta_r(y) = 1 + \sum_{\substack{\beta \in GF(2^{2m}) \\ \beta^{2^m+1} = 1}} \sum_{\substack{\alpha \in GF(2^m) \\ \alpha \neq 0}} (-1)^{Tr_1^{2m}\{(y\alpha\beta + \alpha^r\beta^r)\}}$$

Furthermore, let $r \equiv s \mod 2^m+1$.

$$Tr_1^{2m}(y\alpha\beta + \alpha^r\beta^r) = Tr_1^{2m}(y\alpha\beta + \alpha^{2^k}\beta^s)$$

$$= Tr_1^{2m}\{y\alpha\beta + (\alpha^{2^k}\beta^s)^{2^{n-k}}\}$$

$$= Tr_1^{2m}\{y\alpha\beta + \alpha\beta^{s2^{-k}}\}$$

Substituting this into the above,

$$\Delta_r(y) = 1 + \sum_{\substack{\beta \in GF(2^{2m}) \\ \beta^{2^m+1} = 1}} \sum_{\substack{\alpha \in GF(2^m) \\ \alpha \neq 0}} (-1)^{Tr_1^{2m}\{\alpha(y\beta + \beta^{s2^{-k}})\}}$$

Since there are 2^m+1 (2^m+1)-st roots of unity in $GF(2^{2m})$, the above reduces to:

$$\Delta_r(y) = 1 + \sum_{\beta \in GF(2^{2m})} \sum_{\alpha \in GF(2^m)} (-1)^{Tr_1^{2m}\{\alpha(y\beta + \beta^{s2^{-k}})\}}$$

$$\beta^{2^m+1} = 1$$

$$- (2^m + 1).$$

From Lemma 3-2,

$$Tr_1^{2m}\{\alpha(y\beta + \beta^{s2^{-k}})\}$$

$$= Tr_1^m\{\alpha(y\beta + \beta^{s2^{-k}} + y^{2^m}\beta^{2^m} + \beta^{2^m s2^{-k}})\}$$

$$= Tr_1^m\{\alpha(y\beta + \beta^{s2^{-k}} + y^{2^m}\beta^{-1} + \beta^{-s2^{-k}})\}.$$

Note that $(y\beta + \beta^{s2^{-k}} + y^{2^m}\beta^{-1} + \beta^{-s2^{-k}}) \in GF(2^m)$. Let $N_\beta(y)$ denote the number of distinct solutions β in $GF(2^{2m})$ to (3.9) and (3.10).

$$y\beta + \beta^{s2^{-k}} + y^{2^m}\beta^{-1} + \beta^{-s2^{-k}} = 0 \qquad (3.9)$$

$$\beta^{2^m+1} = 1 \qquad (3.10)$$

where

$$y \in GF(2^{2m}).$$

$$\Delta_r(y) = -2^m + \sum_{\beta \in GF(2^{2m})} \sum_{\alpha \in GF(2^m)} (-1)^{Tr_1^m\{\alpha(y\beta + \beta^{s2^{-k}} + y^{2^m}\beta^{-1} + \beta^{-s2^{-k}})\}}$$

$$\beta^{2^m+1} = 1$$

Then using Lemma 1-1,

$$\Delta_r(y) = -2^m + 2^m N_\beta(y)$$

$$= 2^m\{N_\beta(y) - 1\} \qquad (3.11)$$

QED

Raising (3.9) to the power 2^k, we obtain

$$y^{2^k}\beta^{2^k} + \beta^s + y^{2^{m+k}}\beta^{-2^k} + \beta^{-s} = 0.$$

Multiplying by β^j and raising to the power 2^i for some j and i, the above equation can be transformed to the form:

$$z_1\beta^{e_1} + z_2\beta^{e_2} + z_3\beta^{e_3} + z_4 = 0 \qquad (3.12)$$

where

e_1, e_2 and e_3 are non-negative integers with at least one odd e_i and z_i is some power of y.

Let $e_{max} = \max\{e_1, e_2, e_3\}$. Note that $e_{max} \leq 2\cdot\max\{|s|, 2^k\}$. Then $\Delta_r(y) \leq 2^m(e_{max} - 1)$ since (3.12) can have at most e_{max} roots for β in $GF(2^{2m})$. This upper bound on $\Delta_r(y)$ gives the bound on the minimum weight of the corresponding $(2^{2m}-1,4m)$ cyclic code.

$$w_{min} \geq (2^{2m} + 2^m - e_{max}\cdot 2^m)/2 \qquad (3.13)$$

From (3.11), $\min_y \Delta_r(y) = -2^m$. This gives the upper bound on the weight of the cyclic code.

$$w_{max} \leq (2^{2m} + 2^m)/2 \qquad (3.14)$$

From (3.11), $\Delta_r(y)$ is negative if and only if $N_\beta(y) = 0$. In view of Lemma 2-5, there must exist at least one y in $GF(2^{2m})$ such that $N_\beta(y) = 0$. This implies that the upper bound in (3.14) is always achieved.

Therefore, if $n = 2m$, $GCD(r, 2^n-1) = 1$, $r \equiv 2^k \bmod 2^m-1$ and $r \equiv s \bmod 2^m+1$, the following bounds must hold for $\Delta_r(y)$ and weight w of the corresponding $(2^{2m}-1,4m)$

cyclic code. Furthermore, the lower bound for $\Delta_r(y)$ and the upper bound for w are always attained.

$$-2^m \leq \Delta_r(y) \leq 2^m(e_{max} - 1) \tag{3.15}$$

$$2^{2m-1} + 2^{m-1} - e_{max}\cdot 2^{m-1} \leq w \leq 2^{2m-1} + 2^{m-1} \tag{3.16}$$

e_{max} is itself bounded by:

$$e_{max} \leq 2\cdot\max\{|s|, 2^k\}.$$

We are now in a position to analyze decimations (3.1) through (3.6). They are considered in Theorems 3-6 through 3-11 respectively.

THEOREM 3-6:

If $n \equiv 0 \mod 4$, $n = 2m$ and $r = 2^{m+1} - 1$, $\Delta_r(y)$ is a 4-valued function. Δ_r and $\eta(\Delta_r)$ are given by:

Δ_r	$\eta(\Delta_r)$
2^{m+1}	$(2^{2m-1} - 2^{m-1})/3$
2^m	2^m
0	$2^{2m-1} - 2^{m-1}$
-2^m	$(2^{2m} - 2^m)/3$

proof:

From (2.3), $GCD(r, 2^n-1) = 1$.

$$r = 2(2^m - 1) + 1 \equiv 1 \mod 2^m-1$$

$$r = 2(2^m + 1) - 3 \equiv -3 \mod 2^m+1$$

With $k = 0$, $s = -3$ and $n = 2m$, (3.9) becomes:

$$y\beta + \beta^{-3} + y^{2^m}\beta^{-1} + \beta^3 = 0 \qquad (3.17)$$

Multiplying (3.17) by β^3,

$$\beta^6 + y\beta^4 + y^{2^m}\beta^2 + 1 = 0 \qquad (3.18)$$

Raising (3.18) to the power 2^{-1} or equivalently 2^{n-1}, $N_\beta(y)$ becomes the number of distinct solutions β in $GF(2^{2m})$ to (3.19) and (3.20):

$$\beta^3 + y^{\frac{1}{2}}\beta^2 + y^{2^{m-1}}\beta + 1 = 0 \qquad (3.19)$$

$$\beta^{2^m+1} = 1 \qquad (3.20)$$

Since (3.19) is of degree 3, it can have no root, one root or three roots. Suppose (3.19) has three distinct roots: β_1, β_2 and β_3. Furthermore, suppose β_1 and β_2 satisfy (3.20). Then, since $\beta_1\beta_2\beta_3 = 1$,

$$\beta_3^{2^m+1} = \{(\beta_1\beta_2)^{-1}\}^{2^m+1} = (\beta_1^{2^m}\beta_2^{2^m})^{2^m+1}$$

$$= (\beta_1^{2^m+1})^{2^m}(\beta_2^{2^m+1})^{2^m} = 1.$$

This says that β_3 also satisfies (3.20). Therefore, $N_\beta(y) = 2$ if and only if there exist one repeated root of multiplicity 2 and another root.

Let N_i be the number of times $N_\beta(y) = i$ as y ranges over $GF(2^{2m})$.

Let $f(\beta) = \beta^3 + y^{\frac{1}{2}}\beta^2 + y^{2^{m-1}}\beta + 1$ and $f'(\beta)$ be its formal derivative. From Lemma 3-4, $g(\beta)$ is a repeated factor of $f(\beta)$ if and only if $g(\beta)$ divides $GCD(f(\beta),f'(\beta))$.

$$f'(\beta) = \beta^2 + y^{2^{m-1}}$$

By the Euclid's algorithm, it is easy to show that

$$GCD(f(\beta),f'(\beta)) = \text{constant if } y^{2^m+1} \neq 1 \text{ and}$$

$$GCD(f(\beta),f'(\beta)) = \beta^2 + y^{2^{m-1}} \text{ if } y^{2^m+1} = 1.$$

Hence, $f(\beta)$ has a repeated factor if and only if $y^{2^m+1} = 1$.

Now, let $y^{2^m+1} = 1$ and factor $f(\beta)$.

$$f(\beta) = (\beta + y^{\frac{1}{2}})(\beta + y^{2^{m-2}})^2$$

Note that $f(\beta) = 0$ has a repeated root of multiplicity 3 when $y^{\frac{1}{2}} = y^{2^{m-2}}$ or

$$y = y^{2^{m-1}} \tag{3.21}$$

(3.21) says $y \in GF(2^{m-1})$. Since $y \in GF(2^{2m})$ and $GCD(2m,m-1) = 1$, $y \in GF(2^{2m}) \cap GF(2^{m-1}) = GF(2)$. Hence, $f(\beta) = 0$ has a repeated root of multiplicity 3 if and only if $y = 1$.

Therefore, $f(\beta) = 0$ has one repeated root of multiplicity 2

$$\beta_1 = y^{2^{m-2}} \tag{3.22}$$

and another root

$$\beta_2 = y^{\frac{1}{2}} \tag{3.23}$$

if and only if $y^{2^m+1} = 1$, $y \neq 1$.

The root given by (3.22) satisfies (3.20) since $y^{2^m+1} = 1$. The root given by (3.23) satisfies (3.20) since $y^{2^m+1} = 1$ and 2 does not divide 2^m+1.

Therefore, $N_\beta(y) = 2$ and $\Delta_r(y) = 2^m$ if and only if $y^{2^m+1} = 1$, $y \neq 1$. Since there exist 2^m+1 (2^m+1)-st roots of unity including a unit element in $GF(2^{2m})$, $N_2 = 2^m$.

Using Lemma 2-5, the following equalities must hold.

$$2^{m+1} \cdot N_3 + 2^m 2^m - 2^m \cdot N_0 = 2^{2m} \tag{3.24}$$

$$2^{2m+2} \cdot N_3 + 2^{2m} 2^m + 2^{2m} \cdot N_0 = 2^{4m} \tag{3.25}$$

Dividing (3.24) by 2^m and (3.25) by 2^{2m}, we obtain

$$2 \cdot N_3 - N_0 = 0 \tag{3.26}$$

$$4 \cdot N_3 + N_0 = 2^{2m} - 2^m \tag{3.27}$$

Solving for N_0 and N_3 in (3.26) and (3.27),

$$N_0 = (2^{2m} - 2^m)/3$$

$$N_3 = (2^{2m-1} - 2^{m-1})/3$$

Since $N_0 + N_1 + N_2 + N_3 = 2^{2m}$,

$$N_1 = 2^{2m} - (2^{2m} - 2^m)/3 - 2^m - (2^{2m-1} - 2^{m-1})/3$$

$$= 2^{2m-1} - 2^{m-1}$$ QED

THEOREM 3-7:

If $n = 4m$ and $r = (2^m-1)(2^{2m}+1) + 2$, $\Delta_r(y)$ is a 4-valued function. Δ_r and $\eta(\Delta_r)$ are given by:

Δ_r	$\eta(\Delta_r)$
2^{3m}	2^m
2^{2m}	$2^{4m-1} - 2^{3m-1}$
0	$2^{3m} - 2^m$
-2^{2m}	$2^{4m-1} - 2^{3m-1}$

proof:

From (2.4), $GCD(r, 2^n-1) = 1$.

$$r \equiv 2 \mod 2^{2m}+1$$

$$r = (2^m-1)\{(2^m+1)(2^m-1) + 2\} + 2$$

$$= (2^{2m}-1)(2^m-1) + 2^{m+1}$$

$$\equiv 2^{m+1} \mod 2^{2m}-1$$

With $k = m+1$, $s = 2$ and $n = 4m$, (3.9) becomes:

$$y\beta + \beta^{2\cdot 2^{-m-1}} + y^{2^{2m}}\beta^{-1} + \beta^{-2\cdot 2^{-m-1}} = 0.$$

Or $$y\beta + \beta^{2^{-m}} + y^{2^m}\beta^{-1} + \beta^{-2^{-m}} = 0 \qquad (3.28)$$

(3.10) becomes:

$$\beta^{2^{2m}+1} = 1$$

which implies

$$\beta^{-2^{-m}} = \beta^{2^m} \text{ and } \beta^{2^{-m}} = \beta^{-2^m} \qquad (3.29)$$

Using (3.29), $N_\beta(y)$ is the number of distinct solutions β in $GF(2^{4m})$ to (3.30) and (3.31)

$$y\beta + y^{2^{2m}}\beta^{-1} + (\beta + \beta^{-1})^{2^m} = 0 \qquad (3.30)$$

$$\beta^{2^{2m}+1} = 1 \qquad (3.31)$$

First, consider the case $y \in GF(2^{2m})$. (3.30) becomes:

$$y(\beta + \beta^{-1}) = (\beta + \beta^{-1})^{2^m} \qquad (3.32)$$

Clearly $\beta = 1$ satisfies (3.32) and (3.31). Hence, we now consider the equation:

$$y = (\beta + \beta^{-1})^{2^m-1}, \quad y \in GF(2^{2m}) \qquad (3.33)$$

We will show that

1. There exists no solution to (3.33) and (3.31) if $y = 1$ or $y^{2^m+1} \neq 1$.

2. There exist 2^m distinct solutions to (3.33) and (3.31) if $y^{2^m+1} = 1$, $y \neq 1$.

Raising (3.33) to the power 2^m+1,

$$y^{2^m+1} = (\beta + \beta^{-1})^{2^{2m}-1} = 1.$$

Hence, there is no solution to (3.33) if $y^{2^m+1} \neq 1$.

Next, let $y = 1$ in (3.33).

$$1 = (\beta + \beta^{-1})^{2^m-1} \tag{3.34}$$

This says that $(\beta + \beta^{-1}) = \delta$ for some $\delta \in GF(2^m)$, $\delta \neq 0$.

Multiplying β on both sides,

$$\beta^2 + \delta\beta + 1 = 0. \tag{3.35}$$

Transform (3.35) by introducing a new variable ω:

$$\omega = \delta^{-1}\beta$$

Then $\beta = \delta\omega$ and (3.35) becomes:

$$\delta^2\omega^2 + \delta^2\omega + 1 = 0.$$

Or $$\omega^2 + \omega = \delta^{-2} \tag{3.36}$$

Raising both sides of (3.36) to the power 2^i and adding $i = 0, 1, \ldots, 2m-1$, we obtain:

$$\sum_{i=0}^{2m-1} (\omega^2 + \omega)^{2^i} = \sum_{i=0}^{2m-1} (\delta^{-2})^{2^i}. \tag{3.37}$$

(3.37) reduces to:

$$\omega^{2^{2m}} + \omega = Tr_1^{2m}(\delta^{-2}).$$

Note that

$$Tr_1^{2m}(\delta^{-2}) = Tr_1^{2m}(\delta^{-1}) = 2 \cdot Tr_1^m(\delta^{-1}) = 0$$

since $\delta^{-1} \in GF(2^m)$.

Hence, $\omega \in GF(2^{2m})$. Since $\beta = \delta\omega$, this implies that

$\beta \in GF(2^{2m})$. However, $\beta = 1$ is the only solution to (3.31) in $GF(2^{2m})$. Clearly $\beta = 1$ is not a solution to (3.34). Hence, there is no solution to (3.34) and (3.31).

Now, suppose $y^{2^m+1} = 1$, $y \neq 1$.

Let $y = \omega^{2^m-1}$, $\omega \neq 0$, $\omega \in GF(2^{2m})$. Furthermore, suppose $y = \omega^{2^m-1}$ satisfies (3.33). Then, $y = \delta\omega^{2^m-1}$ satisfies (3.33) for $\delta \in GF(2^m)$, $\delta \neq 0$. Now consider the equation:

$$\beta + \beta^{-1} = \delta\omega. \tag{3.38}$$

Multiplying (3.38) by β on both sides,

$$\beta^2 + \delta\omega\beta + 1 = 0. \tag{3.39}$$

Setting $\beta = (\delta\omega)\lambda$, transform (3.39) to:

$$(\delta\omega)^2\lambda^2 + (\delta\omega)^2\lambda + 1 = 0.$$

Or $$\lambda^2 + \lambda = (\delta\omega)^{-2} \tag{3.40}$$

From Lemma 3-3, (3.40) has 2 solutions for λ and therefore 2 solutions for β to (3.39) and (3.31) if and only if

$$Tr_1^{2m}\{(\delta\omega)^{-2}\} = Tr_1^{2m}\{(\delta\omega)^{-1}\} = 1$$

and $$Tr_1^{4m}\{(\delta\omega)^{-2}\} = 0.$$

Clearly $Tr_1^{4m}\{(\delta\omega)^{-2}\} = 0$ for all $\delta \in GF(2^m)$ and for all $\omega \in GF(2^{2m})$.

Note that

$$Tr_1^{2m}\{(\delta^{-1}\omega^{-1})\} = \begin{cases} 0 \text{ for } 2^{m-1}-1 \text{ choices of } \delta \\ 1 \text{ for } 2^{m-1} \text{ choices of } \delta \end{cases}$$

or $$Tr_1^{2m}\{(\delta^{-1}\omega^{-1})\} = 0 \text{ identically.}$$

Since $Tr_1^{2m}\{(\delta^{-1}\omega^{-1})\} = Tr_1^m\{\delta^{-1}(\omega^{-1} + \omega^{-2^m})\}$, $Tr_1^{2m}\{(\delta^{-1}\omega^{-1})\} = 0$ identically if and only if $\omega^{-1} = \omega^{-2^m}$ or $\omega = \omega^{2^m}$. But

$\omega^{2^m} = \omega$ implies $y = \omega^{2^m-1} = 1$. However, the case $y = 1$ is being excluded. Therefore, there exist $2 \cdot 2^{m-1} = 2^m$ solutions to (3.33) if $y^{2^m+1} = 1$, $y \neq 1$.

To show that solutions of (3.39) satisfy (3.31), suppose $Tr_1^{2m}\{(\delta\omega)^{-1}\} = 1$. Repeatedly raising (3.40) to the powe 2^i and adding $i = 0, 1, \ldots, 2m-1$, we obtain:

$$\sum_{i=0}^{2m-1} (\lambda^2 + \lambda)^{2^i} = \sum_{i=0}^{2m-1} \{(\delta\omega)^{-2}\}^{2^i} \tag{3.41}$$

(3.41) reduces to:

$$\lambda^{2^{2m}} + \lambda = Tr_1^{2m}\{(\delta\omega)^{-1}\} = 1 \tag{3.42}$$

Since $\beta = (\delta\omega)\lambda$, $\beta^{2^{2m}} = (\delta\omega)^{2^{2m}} \lambda^{2^{2m}} = (\delta\omega)\lambda^{2^{2m}}$. Using (3.40) and (3.42),

$$\beta^{2^{2m}+1} = (\delta\omega)^2\lambda(\lambda + 1) = (\lambda^2 + \lambda)^{-1}(\lambda^2 + \lambda) = 1.$$

Hence, for $y \in GF(2^{2m})$

$N_\beta(y) = 2^m+1$ and $\Delta_r(y) = 2^{3m}$ if $y^{2^m+1} = 1$, $y \neq 1$

and $N_\beta(y) = 1$ and $\Delta_r(y) = 0$ otherwise.

In order to finish the proof of Theorem 3-7, we use the result due to Welch.

The system of two equations

$$y\beta + y^{2^{2m}}\beta^{-1} + (\beta + \beta^{-1})^{2^m} = 0$$

$$\beta^{2^{2m}+1} = 1$$

where

$$y \in GF(2^{4m}) - GF(2^{2m})$$

has at most 2 solutions for β in $GF(2^{4m})$.

Again let N_i denote the number of times $N_\beta(y) = i$ as y ranges over $GF(2^{4m})$. Then, from Lemma 2-5, we must have:

$$2^{3m} \cdot 2^m + 2^{2m} \cdot N_2 - 2^{2m} \cdot N_0 = 2^{4m}$$

$$2^{6m} \cdot 2^m + 2^{4m} \cdot N_2 + 2^{4m} \cdot N_0 = 2^{8m}$$

Solving for N_2 and N_0,

$$N_2 = N_0 = 2^{4m-1} - 2^{3m-1}.$$

Hence,

$$N_1 = 2^{4m} - (2^m + N_2 + N_0) = 2^{3m} - 2^m. \qquad \text{QED}$$

THEOREM 3-8:

If $n = 2m$ and $r = 2^m + 3$, $\Delta_r(y)$ is at most a 5-valued function.

$$\Delta_r(y) = 2^m(j-1), \quad 0 \leq j \leq 4.$$

proof:

From (2.5), $GCD(r, 2^n-1) = 1$.

$$r \equiv 2^2 \mod 2^m-1$$

$$r \equiv 2 \mod 2^m+1$$

With $k = 2$, $s = 2$ and $n = 2m$, (3.9) becomes:

$$y\beta + \beta^{2 \cdot 2^{-2}} + y^{2^m}\beta^{-1} + \beta^{-2 \cdot 2^{-2}} = 0.$$

Raising to the power 2^1,

$$y^2\beta^2 + \beta + y^{2^{m+1}}\beta^{-2} + \beta^{-1} = 0.$$

Multiplying by β^2, $N_\beta(y)$ becomes the number of distinct solutions β in $GF(2^{2m})$ to (3.43) and (3.44):

$$y^2\beta^4 + \beta^3 + \beta + y^{2^{m+1}} = 0 \qquad (3.43)$$

$$\beta^{2^m+1} = 1 \tag{3.44}$$

Hence, $\Delta_r(y) = 2^m\{N_\beta(y) - 1\}$ where $N_\beta(y) = 0, 1, 2, 3$ or 4.

QED

A further analysis can be made for this case.

First, consider the case $y \in GF(2^m)$. Since $y^{2^m} = y$, (3.43) becomes:

$$y^2\beta^4 + \beta^3 + \beta + y^2 = 0. \tag{3.45}$$

(3.45) can be factored to become:

$$y^2(\beta + 1)^2(\beta^2 + y^{-2}\beta + 1) = 0. \tag{3.46}$$

Clearly $\beta = 1$ is a solution to (3.46) and (3.44). Now consider the second factor of (3.46):

$$\beta^2 + y^{-2}\beta + 1 = 0 \tag{3.47}$$

(3.47) has either no root or two distinct roots. Transform (3.47) by introducing a new variable ω:

$$\omega = y^2\beta \tag{3.48}$$

Then $\beta = y^{-2}\omega$ and (3.47) becomes:

$$(y^{-2})^2\omega^2 + (y^{-2})^2\omega + 1 = 0. \tag{3.49}$$

Multiplying (3.49) by y^4, we obtain:

$$\omega^2 + \omega = y^4 \tag{3.50}$$

In order to have solutions for ω in (3.50) and hence solutions for β in (3.47) which also satisfy (3.44), we must have:

$$Tr_1^m(y^4) = Tr_1^m(y) = 1$$

and $$Tr_1^{2m}(y^4) = Tr_1^{2m}(y) = 0.$$

This follows again from Lemma 3-3, for if $Tr_1^m(y) = 0$, two roots for ω in (3.50) belong to $GF(2^m)$ and hence two roots for β in (3.47) belong to $GF(2^m)$. But (3.44) has only one solution in $GF(2^m)$, namely $\beta = 1$. Clearly $\beta = 1$ is not a root of (3.47).

Since $Tr_1^{2m}(y) = 0$ for all $y \in GF(2^m)$, (3.47) has two distinct roots for β if and only if $Tr_1^m(y) = 1$.

To show that two roots of (3.47) satisfy (3.44), suppose $Tr_1^m(y) = 1$. Repeatedly raising (3.50) to the power 2^i and adding $i = 0, 1, \ldots, m-1$, we obtain:

$$\sum_{i=0}^{m-1} (\omega^2 + \omega)^{2^i} = \sum_{i=0}^{m-1} (y^4)^{2^i} \tag{3.51}$$

(3.51) reduces to:

$$\omega^{2^m} + \omega = Tr_1^m(y) = 1 \tag{3.52}$$

Since $\beta = y^{-2}\omega$, $\beta^{2^m} = (y^{-2})^{2^m}\omega^{2^m} = y^{-2}\omega^{2^m}$. Using (3.50) and (3.52),

$$\beta^{2^m+1} = (y^{-2})^2\omega\omega^{2^m} = y^{-4}\omega(\omega + 1) = 1.$$

Therefore, for $y \in GF(2^m)$

$$\begin{aligned} &N_\beta(y) = 1 \text{ when } Tr_1^m(y) = 0 \\ \text{and } &N_\beta(y) = 3 \text{ when } Tr_1^m(y) = 1. \end{aligned} \tag{3.53}$$

Next, consider the case $y \in GF(2^{2m}) - GF(2^m)$. Multiplying (3.43) by y^{-2}, we obtain:

$$\beta^4 + y^{-2}\beta^3 + y^{-2}\beta + y^{2(2^m-1)} = 0 \tag{3.54}$$

Suppose (3.54) has 4 distinct roots: β_1, β_2, β_3 and β_4. From (3.54) we have

$$\beta_1\beta_2\beta_3\beta_4 = y^{2(2^m-1)}$$

$$\text{or} \quad \beta_4 = (\beta_1\beta_2\beta_3)^{-1} \cdot y^{2(2^m-1)}$$

Furthermore, suppose β_1, β_2 and β_3 satisfy (3.44). Then,

$$(\beta_1\beta_2\beta_3)^{-1} = (\beta_1\beta_2\beta_3)^{2^m}$$

$$\text{and} \quad \beta_4^{2^m+1} = (\beta_1^{2^m+1} \cdot \beta_2^{2^m+1} \cdot \beta_3^{2^m+1})^{2^m} \cdot y^{2(2^{2m}-1)} = 1$$

Hence, β_4 also satisfies (3.44). This implies that if $N_\beta(y) = 3$, (3.54) must have 2 distinct roots and one repeated root of multiplicity 2.

Assume (3.54) has a repeated root β_1. Dividing (3.54) by $(\beta + \beta_1)^2$, we obtain:

$$(\beta^2 + y^{-2}\beta + \beta_1^2)(\beta + \beta_1)^2 + (\beta_1^2 + 1)y^{-2}\beta$$

$$+ y^{2(2^m-1)} + \beta_1^4 = 0$$

Hence, we must have

$$(\beta_1^2 + 1) = 0 \tag{3.55}$$

$$y^{2(2^m-1)} = \beta_1^4 \tag{3.56}$$

(3.55) says $\beta_1 = 1$, which in turn implies $y^{2^m-1} = 1$ from (3.56). This says $y \in GF(2^m)$.

Hence, if $y \in GF(2^{2m}) - GF(2^m)$,

$$N_\beta(y) \neq 3. \tag{3.57}$$

Finally combining (3.53) and (3.57), we obtain:

$$N_\beta(y) = 3 \text{ and } \Delta_r(y) = 2^{m+1}$$

if and only if $y \in GF(2^m)$ and $Tr_1^m(y) = 1$.

For the case $y \in GF(2^{2m}) - GF(2^m)$, (3.54) can be transformed to a more standard form by introducing a new variable σ:

$$\sigma = (\beta + 1)^{-1} \tag{3.58}$$

Then, the number of distinct solutions β to (3.54) and (3.44) is equal to the number of distinct solutions σ in $GF(2^{2m})$ to the system of two equations:

$$\sigma^4 + \lambda\sigma^2 + \lambda\sigma + \lambda y^2 = 0$$

$$\sigma^{2^m} + \sigma = 1$$

where

$$\lambda = (y + y^{2^m})^{-2}, \quad y \in GF(2^{2m}) - GF(2^m).$$

Furthermore, it is conjectured that the following distribution holds for $m > 2$.

Δ_r	$\eta(\Delta_r)$ for m odd	$\eta(\Delta_r)$ for m even
$3\cdot 2^m$	$(2^{2m-3} - 2^{m-2})/3$	$(2^{2m-3} - 2^{m-1})/3$
2^{m+1}	2^{m-1}	2^{m-1}
2^m	$2^{2m-2} - 2^{m-1}$	2^{2m-2}
0	$(2^{2m} + 5\cdot 2^{m-1})/3$	$(2^{2m} + 2^{m-1})/3$
-2^m	$3(2^{2m-3} - 2^{m-2})$	$(3\cdot 2^{2m-3} - 2^{m-1})$

REMARK: If $n = 2m$ and $r = 2^{2m-1} - 2^{m-1} + 1$, $\Delta_r(y)$ is at most a 5-valued function. For the proof, let $r' = 2^m + 3$. Then,

$$\begin{aligned} 2 \cdot r \cdot r' &= (2^{2m} - 2^m + 2)(2^m + 3) \\ &\equiv (3 - 2^m)(3 + 2^m) \mod 2^{2m}-1 \\ &\equiv 2^3 \mod 2^{2m}-1. \end{aligned}$$

The desired result follows directly from Lemma 2-3 and Theorem 3-8.

As an alternative proof, consider the following. For this decimation r, it is easy to show that $r \equiv 1 \mod 2^m-1$, $r \equiv 2 \mod 2^m+1$ and hence $GCD(r, 2^{2m}-1) = 1$. With $k = 0$, $s = 2$ and $n = 2m$, (3.9) becomes:

$$y\beta + \beta^2 + y^{2^m}\beta^{-1} + \beta^{-2} = 0$$

Multiplying the above by β^2, we get:

$$\beta^4 + y\beta^3 + y^{2^m}\beta + 1 = 0$$

Therefore, $\Delta_r(y) = 2^m(j-1)$, $0 \leq j \leq 4$.

THEOREM 3-9;

If $n \equiv 2 \mod 4$, $n = 2m$ and $r = 2^m + 2^{m-1} - 1$, $\Delta_r(y)$ is at most a 6-valued function.

$$\Delta_r(y) = 2^m(j-1), \quad 0 \leq j \leq 5.$$

proof:

From (2.6), $GCD(r, 2^n-1) = 1$.

$$r \equiv 2^{m-1} \mod 2^m-1$$

$$r \equiv 2^{m-1} - 2 \mod 2^m+1$$

With $k = m-1$, $s = 2^{m-1}-2$ and $n = 2m$, (3.9) becomes:

$$y\beta + \beta^{(2^{m-1}-2)2^{-m+1}} + y^{2^m}\beta^{-1} + \beta^{-(2^{m-1}-2)2^{-m+1}}$$

$$= y\beta + \beta^{1-2^{-m+2}} + y^{2^m}\beta^{-1} + \beta^{-(1-2^{-m+2})} = 0$$

Since $\beta^{2^m} = \beta^{-1}$ and $\beta = \beta^{-2^m}$,

$$y\beta + \beta(\beta^{2^m})^{2^{-m+2}} + y^{2^m}\beta^{-1} + \beta^{-1}(\beta^{-2^m})^{2^{-m+2}}$$

$$= y\beta + \beta\cdot\beta^{2^2} + y^{2^m}\beta^{-1} + \beta^{-1}\cdot\beta^{-2^2}$$

$$= y\beta + \beta^5 + y^{2^m}\beta^{-1} + \beta^{-5} = 0$$

Multiplying by β^5,

$$\beta^{10} + y\beta^6 + y^{2^m}\beta^4 + 1 = 0$$

Raising to the power 2^{-1},

$$\beta^5 + y^{\frac{1}{2}}\beta^3 + y^{2^{m-1}}\beta^2 + 1 = 0 \qquad \text{QED}$$

THEOREM 3-10:

If $n = 2m$ and $r = 2^{m+2} - 3$, $\Delta_r(y)$ is at most an 8-valued function.

$$\Delta_r(y) = 2^m(j-1),\ 0 \leq j \leq 7.$$

proof:

From (2.7), $GCD(r, 2^n-1) = 1$.

$$r = 4(2^m-1) + 1 \equiv 1 \mod 2^m-1$$

$$r = 4(2^m+1) - 7 \equiv -7 \mod 2^m+1$$

With $k = 0$, $s = -7$ and $n = 2m$, (3.9) becomes:

$$y\beta + \beta^{-7} + y^{2^m}\beta^{-1} + \beta^7 = 0$$

Multiplying by β^7,

$$\beta^{14} + y\beta^8 + y^{2^m}\beta^6 + 1 = 0$$

Raising to the power 2^{-1},

$$\beta^7 + y^{\frac{1}{2}}\beta^4 + y^{2^{m-1}}\beta^3 + 1 = 0 \qquad \text{QED}$$

REMARK: Computed results indicate that for $n = 2m = 4m'$ and $r = 2^{m+2} - 3$, $\Delta_r(y)$ is at most 5-valued.

$$\Delta_r(y) = 2^m(j-1), \quad j = 0, 1, 2, 3 \text{ or } 5.$$

REMARK: When $n = 8$, a further improvement can be made on Theorem 3-10.

$$r = 2^{4+2} - 3 = 61$$

$$r^{-1} = 23 \cdot 2$$

Let $r' = 23$. Then $r' \equiv 2^3 \mod 15$ and $r' \equiv 6 \mod 17$.

With $k = 3$, $s = 6$ and $n = 2 \cdot 4$, (3.9) becomes:

$$y\beta + \beta^{6 \cdot 2^{-3}} + y^{2^4}\beta^{-1} + \beta^{-6 \cdot 2^{-3}} = 0$$

$$y\beta + \beta^{3 \cdot 2^{-2}} + y^{2^4}\beta^{-1} + \beta^{-3 \cdot 2^{-2}} = 0$$

Since $\beta^{17} = 1$, $\beta^{-1} = \beta^{2^4}$ and $\beta = \beta^{-2^4}$.

$$y\beta + (\beta^{-2^4})^{3 \cdot 2^{-2}} + y^{2^4}\beta^{-1} + (\beta^{2^4})^{3 \cdot 2^{-2}} = 0$$

$$y\beta + \beta^{-12} + y^{16}\beta^{-1} + \beta^{12} = 0$$

$$y\beta + \beta^5 + y^{16}\beta^{-1} + \beta^{-5} = 0$$

Multiplying by β^5 and then raising to the power 2^{-1},

$$\beta^5 + y^{\frac{1}{2}}\beta^3 + y^8\beta^2 + 1 = 0$$

Hence,

$$\Delta_{23}(y^{-61}) = \Delta_{61}(y) = 2^4(j-1), \quad 0 \leq j \leq 5.$$

THEOREM 3-11:

If $n = 2m$ and $r = 2^{m+2} + 2^m - 3$, $\Delta_r(y)$ is at most a 9-valued function.

$$\Delta_r(y) = 2^m(j-1),\ 0 \leq j \leq 8.$$

proof:

From (2.8), $GCD(r, 2^n-1) = 1$.

$$r = 5(2^m - 1) + 2 \equiv 2 \mod 2^m-1$$

$$r = 5(2^m + 1) - 8 \equiv -2^3 \mod 2^m+1$$

With $k = 1$, $s = -2^3$ and $n = 2m$, (3.9) becomes:

$$y\beta + \beta^{-2^3 \cdot 2^{-1}} + y^{2^m}\beta^{-1} + \beta^{2^3 \cdot 2^{-1}} = 0$$

$$y\beta + \beta^{-4} + y^{2^m}\beta^{-1} + \beta^4 = 0$$

Multiplying by β^4,

$$\beta^8 + y\beta^5 + y^{2^m}\beta^3 + 1 = 0 \qquad \text{QED}$$

3. COMPUTED RESULTS

Table 3-1 gives the cyclotomic coset leaders given by (3.1) through (3.6), which are considered in Theorems 3-6 through 3-11 respectively. Table 3-2 gives the actual values of $N_\beta(y) = \{\Delta_r(y)/2^m + 1\}$. It is observed that the bounds given by Theorems 3-8 and 3-9 are tight whereas the bounds given by Theorems 3-10 and 3-11 are not.

For $n = 12$ and $n = 14$, there exist many other decimations which are not covered by 6 theorems of the previous section. Degrees of (3.9) that result from those decimations are found to be high. However, the computed

results indicate that values which $\Delta_r(y)$ takes on are restricted. With 2 exceptions, r = 331 and r = 631 for n = 12, $\Delta_r(y)$ for which $r \equiv 2^k \mod 2^{n/2}-1$ are seen to be 7-valued or less. Table 3-3 lists all decimations of this type for n = 4 through n = 14. The number in parentheses following decimation r is the number of distinct values that $\Delta_r(y)$ takes on.

CYCLOTOMIC COSET LEADERS GIVEN BY (3.1) THROUGH (3.6)

n	4	6	8	10	12	14	16
r_1	7		31		127		511
r_2	7		53		457		3857
r_3	7	11	19	35	67	131	259
r_4		11		47		191	
r_5	7	23	61	125	253	509	1021
r_6		11	53	157	317	637	1277

TABLE 3-1

NUMBER OF SOLUTIONS TO (3.9) and (3.10), $N_\beta(y)$

r_1	0 1 2 3	
r_2	0 1 2 $2^{n/4}+1$	
r_3	0 1 2 3 4	for $n \geq 6$
r_4	0 1 2 3 4	for n = 6
	0 1 2 3 4 5	for n = 10, 14
r_5	0 1 2 3	for n = 4
	0 1 2 3 4	for n = 6
	0 1 2 3 5	for n = 8, 12, 16
	0 1 2 3 4 5	for n = 10, 14
r_6	0 1 2 3 4	for n = 6, 10
	0 1 2 5	for n = 8
	0 1 2 3 4 5 6	for n = 12, 14

TABLE 3-2

DECIMATIONS OF TYPE 2^k MOD $2^{n/2}-1$

n = 4	7(4)				
n = 6	11(5)	23(5)			
n = 8	19(5)	23(5)	31(4)	47(5)	53(4)
	61(5)	91(4)			
n = 10	35(5)	47(6)	95(5)	101(5)	109(6)
	125(6)	157(5)	221(6)	343(6)	
n = 12	67(5)	71(6)	79(7)	127(4)	191(5)
	197(7)	253(5)	317(7)	319(7)	331(8)
	347(7)	379(7)	443(7)	457(4)	473(7)
	599(5)	631(8)	701(6)	757(6)	821(7)
	823(7)	827(7)	1387(4)		
n = 14	131(5)	143(7)	191(6)	383(5)	389(7)
	397(6)	413(6)	445(6)	509(6)	637(7)
	667(7)	763(6)	893(7)	905(7)	953(6)
	1145(7)	1147(7)	1151(6)	1175(6)	1207(6)
	1271(6)	1399(6)	1405(6)	1429(6)	1525(7)
	1655(7)	1715(6)	1907(6)	1909(6)	1913(7)
	2429(6)	2477(7)	2669(6)	2671(7)	2675(7)
	2683(6)	2731(6)	2923(7)	3431(6)	3437(7)
	3445(6)				

TABLE 3-3

CHAPTER IV

MULTI-VALUED CROSS-CORRELATION FUNCTIONS II

1. $\Delta_r(y)$ FOR $r = (2^{mk}+1)/(2^k+1)$

In this chapter we consider $\Delta_r(y)$ for the case

$r = (2^{mk}+1)/(2^k+1)$, m and n/GCD(n,k) both odd.

From Lemma 2-8, $GCD(r,2^n-1) = 1$. It can be shown that $\Delta_r(y)$ is restricted to the form:

$$\Delta_r(y) = 0, \pm 2^{(n+de)/2}$$

where

$$e = GCD(n,k)$$

and d is a some positive odd integer.

Given $r = (2^{mk}+1)/(2^k+1)$

$$= 2^{(m-1)k} - 2^{(m-2)k} + \ldots - 2^k + 1,$$

consider $q = \{2^{m(n-k)}+1\}/\{2^{(n-k)}+1\}$

$$= 2^{-(m-1)k}\{2^{(m-1)n} - 2^k 2^{(m-2)n} + 2^{2k} 2^{(m-3)n} - \ldots - 2^{(m-2)k} 2^n + 2^{(m-1)k}\}$$

$$\equiv 2^{-(m-1)k}\{1 - 2^k + 2^{2k} - \ldots + 2^{(m-1)k}\} \mod 2^n-1.$$

This says that r and q belong to the same proper cyclotomic coset. Hence, to determine $\Delta_r(y)$ for some k, it suffices to consider only those k such that $2k \leq n$ for n odd and $2k \leq (n-2)$ for n even. Furthermore, note that

$$2^{m+jn} \equiv 2^m \mod 2^n-1$$

$$\{2^{(n-m)k}+1\}/(2^k+1) \equiv 2^{-mk}(1+2^{mk})/(2^k+1) \mod 2^n-1$$

Therefore, in determining $\Delta_r(y)$, it suffices to consider

$$3 \leq m \leq n/2,\ 2k \leq n-2 \quad \text{for } n \text{ even}$$
$$\text{and } 3 \leq m \leq n,\ \ 2k \leq n \quad \text{for } n \text{ odd.} \tag{4.1}$$

The case m = 3 reduces to the Welch's case, Theorem 1-6. The case m = n odd is considered in Lemma 2-9. The case in which $3m \equiv \pm 1 \mod n$ and GCD(3,n) = 1 is considered in Lemma 2-10.

In CHAPTER II it was shown that if GCD(3,n) = 1, the multiplicative inverse of $r = (2^{3k}+1)/(2^k+1)$ can be given by $r'' = 2^s(2^{mt}+1)/(2^t+1)$ for some s where m and t are given by (2.9) and (2.10) respectively. Similarly, if GCD(m,n) = 1, the multiplicative inverse of $r = (2^{mk}+1)/(2^k+1) \mod 2^n-1$ can be given by

$$r'' = 2^s(2^{m''k''}+1)/(2^{k''}+1) \text{ for some } s$$

where

$$m \cdot m' \equiv 1 \mod n$$

$$j \equiv m \cdot k \mod n$$

$$m'' = \begin{cases} n - m' & \text{when } m' \text{ is even} \\ m' & \text{when } m' \text{ is odd} \end{cases}$$

$$\text{and } k'' = \begin{cases} n - j & \text{when } j > (n-1)/2 \\ j & \text{when } j \leq (n-1)/2 \end{cases}$$

For the analysis of $\Delta_r(y)$ of this type, we follow the same arguments used by Welch when he proved Theorem 1-6.

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr_1^n\{xy + x^{(2^{mk}+1)/(2^k+1)}\}}$$

From Lemma 2-7, $GCD(2^k+1, 2^n-1) = 1$. Hence, a mapping

$x \to x^{2^k+1}$ permutes elements of $GF(2^n)$. Then,

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr_1^n\{yx^{2^k+1} + x^{2^{mk}+1}\}}$$

Let $e = GCD(n,k)$. Then, it is easy to show that

$$Tr_1^n(x) = Tr_1^e\{Tr_e^n(x)\}$$

Let $x \in GF(2^n)$. Then, the element x can be expressed in the form

$$x = \sum_{i=1}^{n/e} x_i \sigma_i$$

where

$$x_i \in GF(2^e)$$

$$\sigma_i \in GF(2^n)$$

and $\{\sigma_1, \sigma_2, \ldots, \sigma_{n/e}\}$ is the basis of $GF(2^n)$ over $GF(2^e)$.

Then,

$$Tr_1^n(x) = Tr_1^n\{\sum_{i=1}^{n/e} x_i \sigma_i\}$$

$$= Tr_1^e\{Tr_e^n\{\sum_{i=1}^{n/e} x_i \sigma_i\}\}$$

$$= Tr_1^e\{\sum_{i=1}^{n/e} x_i Tr_e^n(\sigma_i)\}$$

Expanding $x^{2^{mk}+1}$,

$$x^{2^{mk}+1} = \{\sum_{i=1}^{n/e} x_i \sigma_i\}^{2^{mk}} \{\sum_{j=1}^{n/e} x_j \sigma_j\}$$

$$= \{\sum_{i=1}^{n/e} x_i^{2^{mk}} \sigma_i^{2^{mk}}\} \sum_{j=1}^{n/e} x_j \sigma_j$$

$$= \{\sum_{i=1}^{n/e} x_i \sigma_i^{2^{mk}}\} \sum_{j=1}^{n/e} x_j \sigma_j$$

$$= \sum_{i,j} x_i x_j \sigma_i^{2^{mk}} \sigma_j$$

Define Q(x) by:

$$Q(x) = Tr_e^n(yx^{2^k+1} + x^{2^{mk}+1})$$

where

$$y \in GF(2^n).$$

$$Q(x) = Tr_e^n\{y \cdot \sum_{i,j} x_i x_j \sigma_i^{2^k} \sigma_j + \sum_{i,j} x_i x_j \sigma_i^{2^{mk}} \sigma_j\}$$

$$= Tr_e^n\{\sum_{i,j} x_i x_j (y\sigma_i^{2^k} \sigma_j + \sigma_i^{2^{mk}} \sigma_j)\}$$

$$= \sum_{i,j} x_i x_j \, Tr_e^n(y\sigma_i^{2^k} \sigma_j + \sigma_i^{2^{mk}} \sigma_j)$$

$$= \sum_{i,j} x_i x_j \cdot \delta_{ij}$$

where

$$\delta_{ij} = Tr_e^n(y\sigma_i^{2^k} \sigma_j + \sigma_i^{2^{mk}} \sigma_j) \in GF(2^e).$$

Hence, Q(x) is a quadratic form over $GF(2^e)$.

A quadratic form with coefficients in $GF(2^e)$ can be reduced to one of the following 2 canonical forms: [20] [21]

Type I: $QF = x_1x_2 + \ldots + x_{2s-1}x_{2s} + x_{2s+1}^2$

Type II: $QF_\lambda = x_1x_2 + \ldots + x_{2s-1}x_{2s} + \lambda(x_{2s-1}^2 + x_{2s}^2)$

where

$\lambda = 0$

or $\lambda \in GF(2^e)$ and $Tr_1^e(\lambda) = 1$.

First, consider $\Delta_r(y)$ for Type I.

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr_1^e\{Q(x)\}}$$

$$= \sum_{x_1} \cdots \sum_{x_{n/e}} (-1)^{Tr_1^e(x_1x_2 + x_3x_4 + \cdots + x_{2s+1}^2)}$$

where

x_i's range over $GF(2^e)$.

$$\Delta_r(y) = \sum_{x_1} \sum_{x_2} (-1)^{Tr_1^e(x_1x_2)} \sum_{x_3} \sum_{x_4} (-1)^{Tr_1^e(x_3x_4)} \cdots$$

$$\sum_{x_{2s-1}} \sum_{x_{2s}} (-1)^{Tr_1^e(x_{2s-1}x_{2s})} \sum_{x_{2s+1}} (-1)^{Tr_1^e(x_{2s+1}^2)}$$

$$\sum_{x_{2s+2}} \cdots \sum_{x_{n/e}} (1)$$

From Lemma 1-1,

$$\sum_{x_{2s+1}} (-1)^{Tr_1^e(x_{2s+1}^2)} = \sum_{x_{2s+1}} (-1)^{Tr_1^e(x_{2s+1})} = 0$$

Hence, if Q(x) is of Type I, $\Delta_r(y) = 0$.

Next, consider $\Delta_r(y)$ for Type II.

$$\Delta_r(y) = \sum_{x_1} \sum_{x_2} (-1)^{Tr_1^e(x_1x_2)} \sum_{x_3} \sum_{x_4} (-1)^{Tr_1^e(x_3x_4)} \cdots$$

$$\sum_{x_{2s-1}} \sum_{x_{2s}} (-1)^{Tr_1^e\{x_{2s-1}x_{2s} + \lambda(x_{2s-1}^2 + x_{2s}^2)\}}$$

$$\sum_{x_{2s+1}} \cdots \sum_{x_{n/e}} (1)$$

Consider the s-th sum. By the substitution of

$x_{2s-1} \to (x_{2s-1} + \lambda^{1/2})$ and $x_{2s} \to (x_{2s} + \lambda^{1/2})$, the exponent of the s-th sum becomes:

$$\begin{aligned} & Tr_1^e\{(x_{2s-1} + \lambda^{1/2})(x_{2s} + \lambda^{1/2}) + \lambda(x_{2s-1}^2 + \lambda + x_{2s}^2 + \lambda)\} \\ &= Tr_1^e\{x_{2s-1}x_{2s} + \lambda + \lambda^{1/2}(x_{2s-1} + x_{2s}) + \lambda(x_{2s-1}^2 + x_{2s}^2)\} \\ &= Tr_1^e(x_{2s-1}x_{2s} + \lambda) \end{aligned}$$

Then the s-th sum becomes:

$$(-1)^{Tr_1^e(\lambda)} \sum_{x_{2s-1}} \sum_{x_{2s}} (-1)^{Tr_1^e(x_{2s-1}x_{2s})}$$

Hence,

$$\Delta_r(y) = (-1)^{Tr_1^e(\lambda)} \{\sum_{x_1} \sum_{x_2} (-1)^{Tr_1^e(x_1x_2)}\}^s$$

$$\sum_{x_{2s+1}} \cdots \sum_{x_{n/e}} (1)$$

Since

$$\sum_{x_1} \sum_{x_2} (-1)^{Tr_1^e(x_1x_2)} = 2^e$$

and $$\sum_{x_{2s+1}} \cdots \sum_{x_{n/e}} (1) = (2^e)^{n/e - 2s} = 2^{n-2es},$$

we have

$$\Delta_r(y) = (-1)^{Tr_1^e(\lambda)} (2^e)^s \cdot 2^{n-2es} = \pm 2^{n-es}$$

Thus we have:

$$\begin{aligned} &\text{If } Q(x) \text{ is of Type I, } \Delta_r(y) = 0 \\ &\text{If } Q(x) \text{ is of Type II, } \Delta_r(y) = \pm 2^{n-es} \end{aligned} \qquad (4.2)$$

where

$2s$ is the rank of QF_λ.

In order to evaluate $\Delta_r(y)$ explicitly, it suffices to find the rank of the quadratic form over $GF(2^e)$ of the Type II, QF_λ.

Suppose an element z in $GF(2^n)$ has its first $2s$ coordinates equal to zero in that coordinates which produced the canonical form. Then

$$Q(x + z) = Q(x) + Q(z), \quad x \in GF(2^n).$$

Furthermore, if the quadratic form is of Type II, $Q(z) = 0$. Hence, to find the rank of the quadratic form of Type II, we must find the number of z in $GF(2^n)$ such that

$$\begin{aligned}
0 &= Q(x + z) + Q(x) \\
&= Tr_e^n\{y(x+z)^{2^k+1} + (x+z)^{2^{mk}+1}\} \\
&\quad + Tr_e^n\{yx^{2^k+1} + x^{2^{mk}+1}\} \\
&= Tr_e^n\{yx^{2^k+1} + yx^{2^k}z + yxz^{2^k} + yz^{2^k+1} + x^{2^{mk}+1} \\
&\quad + x^{2^{mk}}z + xz^{2^{mk}} + z^{2^{mk}+1} + yx^{2^k+1} + x^{2^{mk}+1}\} \\
&= Tr_e^n\{yx^{2^k}z + yxz^{2^k} + x^{2^{mk}}z + xz^{2^{mk}}\} \\
&\quad + Tr_e^n\{yz^{2^k+1} + z^{2^{mk}+1}\} \\
&= Tr_e^n\{y^{2^{(m-1)k}}x^{2^{mk}}z^{2^{(m-1)k}} + y^{2^{mk}}x^{2^{mk}}z^{2^{(m+1)k}} \\
&\quad + x^{2^{mk}}z + x^{2^{mk}}z^{2^{2mk}}\} + Q(z)
\end{aligned}$$

$$= Tr_e^n\{x^{2^{mk}}\{z^{2^{2mk}} + z + y^{2^{mk}} z^{2^{(m+1)k}} + y^{2^{(m-1)k}} z^{2^{(m-1)k}}\}\}$$

Since the above must hold as x ranges over $GF(2^n)$, we must have

$$z^{2^{2mk}} + z + y^{2^{mk}} z^{2^{(m+1)k}} + y^{2^{(m-1)k}} z^{2^{(m-1)k}} = 0 \quad (4.3)$$

Suppose z_1 is a solution to (4.3). Then, for $\alpha_1 \in GF(2^e)$, $z = \alpha_1 z_1$ is also a solution to (4.3) since

$$z^{2^{jk}} = \alpha_1^{2^{jk}} z_1^{2^{jk}} = \alpha_1 \cdot z_1^{2^{jk}} \quad \text{for any } j.$$

If z_2 is another solution to (4.3), then for $\alpha_2 \in GF(2^e)$ $z = (\alpha_1 z_1 + \alpha_2 z_2)$ is also a solution to (4.3). This says that the set of solutions to (4.3) is a linear space over $GF(2^e)$. Hence, the number of solutions z in $GF(2^n)$ to (4.3) is of the form $(2^e)^d$, where d is the dimension of the solution space over $GF(2^e)$.

The rank of the quadratic form of Type II over $GF(2^e)$, 2s, is equal to:

$$2s = n/e - d \quad (4.4)$$

Since n/e is odd, d must also be odd.

It can be shown that if $\{z_1, z_2, \ldots, z_{n/e}\}$ is the basis for $GF(2^n)$ over $GF(2^e)$, then $\{z_1, z_2, \ldots, z_{n/e}\}$ is also the basis of $GF(2^{2kn/e})$ over $GF(2^{2k})$.

The set of solutions to (4.3) is also a linear space over $GF(2^{2k})$. In view of the fact that (4.3) is of

degree $2^{2mk} = (2^{2k})^m$, the dimension of the solution space is at most m. Hence,

$$1 \leq d \leq m, \quad d \text{ odd} \tag{4.5}$$

Substituting (4.4) into (4.2), we have

$$\Delta_r(y) = \begin{cases} 0 \\ \pm 2^{(n+de)/2}, \end{cases} \quad 1 \leq d \leq m, \quad d \text{ odd} \tag{4.6}$$

In [22] Kasami evaluates the weight distribution of the dual of the cyclic code whose generator polynomial is

$$\prod_{i=0}^{u-1} f_{1+2^{k(2i+1)}}(x).$$

The weight of this code is restricted to the form:

$$2^{n-1} \pm 2^{(n-e)/2 + ie - 1} \qquad 1 \leq i \leq u-1$$

where

$$e = \text{GCD}(n,k).$$

The $(2^n-1, 2n)$ cyclic code generated by

$$\frac{x^{2^n-1} + 1}{x^{2n} \cdot f_{1+2^k}(1/x) \cdot f_{1+2^{mk}}(1/x)}$$

is a subcode of the Kasami's code for $u = (m+1)/2$. Hence the weight restriction implies that (4.6) can be improved to:

$$\Delta_r(y) = \begin{cases} 0 \\ \pm 2^{(n+de)/2}, \end{cases} \quad 1 \leq d \leq m-2, \quad d \text{ odd} \tag{4.7}$$

(4.7) immediately implies that

LEMMA 4-1:

If $r = (2^{5k}+1)/(2^k+1)$, $e = \text{GCD}(n,k)$ and n/e is odd,

$\Delta_r(y)$ is at most 5-valued.

$$\Delta_r(y) = 0, \pm 2^{(n+e)/2}, \pm 2^{(n+3e)/2}.$$

2. COMPUTED RESULTS AND CONJECTURES

Table 4-1 lists the cyclotomic coset leaders given by $r = (2^{mk}+1)/(2^k+1)$ where both m and n/GCD(n,k) are odd. m and k are restricted to (4.1). The number in parentheses following decimation r is the number of the distinct values that $\Delta_r(y)$ takes on. For n =15, the coset leaders given by m = 15 are omitted from Table 4-1.

These results exhibit definite patterns and they can be summarized by the following 3 conjectures. As before, $e = GCD(n,k)$ and $r = (2^{mk}+1)/(2^k+1) \not\equiv 2^j \mod 2^n-1$ for any j, $0 \leq j \leq n-1$, with m and n/e both odd.

CONJECTURE 4-2:

If $e > 1$, then $\Delta_r(y)$ is a 3-valued function. Δ_r and $n(\Delta_r)$ are given by (1.8).

CONJECTURE 4-3:

If $e = 1$ but n is not a prime, then $\Delta_r(y)$ is at most a 5-valued function. $\Delta_r(y)$ is of the form (4.7).

CONJECTURE 4-4:

If n is a prime, $\Delta_r(y)$ is at most a 5-valued function.

$$\Delta_r(y) = 0, \pm 2^{(n+1)/2}, \pm 2^{(n+3)/2}.$$

REMARK: It is observed that $\Delta_r(y)$ given in Conjecture 4-4 is a 5-valued function if m is restricted to

$$5 \leq m \leq n-2$$

and $3m \not\equiv \pm 1 \mod n$.

Next, we give conjectures on decimations of the types not considered in this chapter. Among the decimations that lead to the 3-valued $\Delta_r(y)$, there remain only a few cases that are not covered by Theorems 1-5, 1-6 or Lemmas 2-9, 2-10. They are listed in Table 1-2. It is seen that they are still not covered by Conjecture 4-2. The following conjecture covers all of these remaining cases.

CONJECTURE 4-5:

The following 5 decimations lead to the 3-valued $\Delta_r(y)$.

(1)	$r = 2^{(n-1)/2} + 3$	$n \equiv 1 \mod 2$
(2)	$r = 2^{(n-1)/2} + 2^{(n-1)/4} - 1$	$n \equiv 1 \mod 4$
(3)	$r = 2^{(n-1)/2} + 2^{(3n-1)/4} - 1$	$n \equiv 3 \mod 4$
(4)	$r = 2^{(n+2)/2} + 3$	$n \equiv 2 \mod 4$
(5)	$r = 2^{n/2} + 2^{(n+2)/4} + 1$	$n \equiv 2 \mod 4$

Δ_r and $\eta(\Delta_r)$ for (1), (2) and (3) are given by (1.8) with $e = 1$. Δ_r and $\eta(\Delta_r)$ for (4) and (5) are given by (1.8) with $e = 2$.

REMARK: The case (1) has been known for some time by Welch.

It is of interest to note that all 3 decimations of Conjecture 4-5 for n odd are of the form $2^{(n-1)/2} + 2^j - 1$ for some j. The next conjecture is on the 5-valued $\Delta_r(y)$.

CONJECTURE 4-6:

The following 5 decimations lead to at most the 5-valued $\Delta_r(y)$.

(1) $r = 2^{(n+1)/2} - 2^{(n-3)/2} \pm 1$ $\quad n \equiv 1 \mod 2$

(2) $r = 2^{(n+3)/4} + 3$ $\quad n \equiv 1 \mod 4$

(3) $r = 2^{(n+1)/2} - 2^{(n+3)/4} + 1$ $\quad n \equiv 1 \mod 4$

(4) $r = 2^{(n-1)/2} - 2^{(n+1)/4} + 1$ $\quad n \equiv 3 \mod 4$

(5) $r = 2^{n/2+2} - 3$ $\quad n \equiv 0 \mod 4$

Conjectures 4-2 through 4-6 have been verified for $n \leq 16$. Conjecture 4-4 with k = 1 and m = 5, 7 & 9, Conjecture 4-5 (1) & (2) and Conjecture 4-6 (2) still hold for n = 17.

CYCLOTOMIC COSET LEADERS GIVEN BY $(2^{mk}+1)/(2^{k}+1)$

n	k	e	m				
			3	5	7	9	11
3	1	1	3(3)				
5	1	1	3(3)	11(3)			
	2	1	11(3)	7(3)			
6	2	2	13(3)				
7	1	1	3(3)	11(3)	43(3)		
	2	1	13(3)	29(3)	27(3)		
	3	1	23(3)	43(3)	15(3)		
9	1	1	3(3)	11(5)	43(5)	171(3)	
	2	1	13(3)	107(5)	109(5)	103(3)	
	3	3	57(3)	1(2)	1(2)	57(3)	
	4	1	47(3)	109(5)	93(5)	31(3)	
10	2	2	13(3)	205(3)			
	4	2	79(3)	181(3)			
11	1	1	3(3)	11(5)	43(3)	171(5)	683(3)
	2	1	13(3)	205(5)	413(3)	423(5)	411(3)
	3	1	57(3)	235(5)	683(3)	343(5)	231(3)
	4	1	143(3)	121(5)	151(3)	429(5)	365(3)
	5	1	95(3)	221(5)	315(3)	189(5)	63(3)
12	4	4	241(3)	1(2)			

n	k	e	m					
			3	5	7	9	11	13
13	1	1	3(3)	11(5)	43(5)	171(3)	683(5)	2731(3)
	2	1	13(3)	205(5)	1643(5)	1691(3)	1645(5)	1639(3)
	3	1	57(3)	919(5)	1367(5)	2731(3)	939(5)	911(3)
	4	1	241(3)	497(5)	483(5)	723(3)	1461(5)	1453(3)
	5	1	287(3)	745(5)	869(5)	1245(3)	749(5)	1243(3)
	6	1	191(3)	445(5)	953(5)	635(3)	381(5)	127(3)
14	2	2	13(3)	205(3)	3277(3)			
	4	2	241(3)	979(3)	2893(3)			
	6	2	319(3)	1339(3)	2773(3)			
15	1	1	3(3)	11(5)	43(5)	171(5)	683(5)	2731(5)
	2	1	13(3)	205(5)	3277(5)	6557(5)	6605(5)	6567(5)
	3	3	57(3)	3641(3)	57(3)	1(2)	1(2)	57(3)
	4	1	241(3)	1943(5)	5783(5)	5813(5)	5805(5)	2895(5)
	5	5	993(3)	1(2)	1(2)	993(3)	1(2)	1(2)
	6	3	575(3)	3529(3)	575(3)	1(2)	1(2)	575(3)
	7	1	383(3)	893(5)	1913(5)	2295(5)	1275(5)	765(5)

TABLE 4-1

CHAPTER V

SUMMARY AND COMMENTS

We have considered the cross-correlation function between two maximal linear recursive sequences: $\{a_i\}_{i=0}^{2^n-2}$ and $\{a_{ri}\}_{i=0}^{2^n-2}$. We have defined the cross-correlation function $\Delta_r(y)$ by:

$$\Delta_r(y) = \sum_{x \in GF(2^n)} (-1)^{Tr(xy + x^r)}$$

and analyzed $\Delta_r(y)$ for two types of decimation r:

(1) $r \equiv 2^k \mod 2^{n/2}-1$

and (2) $r = (2^{mk}+1)/(2^k+1)$.

For the type (1) $\Delta_r(y)$ is of the form:

$$\Delta_r(y) = 2^{n/2}(j-1),\ 0 \leq j \leq J, \text{ for some } J.$$

The value j is the number of distinct solutions to the two equations over $GF(2^n)$. For the type (2) $\Delta_r(y)$ is of the form:

$$\Delta_r(y) = 0, \pm 2^{(n+de)/2},\ 1 \leq d \leq m-2,\ d \text{ odd and } e = GCD(n,k).$$

The value d depends on the rank of the quadratic form over $GF(2^e)$.

For the both types the complete evaluation of $\eta(\Delta_r)$ depends on one's ability to determine the number of solutions to equations in $GF(2^n)$. However, using Lemma 2-5, $\eta(\Delta_r)$ can be determined completely even though

$n(\Delta_r)$ may be known only for certain Δ_r as in the case of Theorems 3-6 and 3-7. For $r = 2^m+3$, $n = 2m$ (Theorem 3-8), $n(\Delta_r)$ can be determined completely if it is possible to

1. evaluate $\Sigma\{\Delta_r(y)\}^3$

or 2. find any one of N_0, N_1, N_2 and N_4 where N_i is the number of times $N_\beta(y) = i$.

From the observation of results obtained, it is seen that many decimations that lead to 3-valued, 4-valued and 5-valued $\Delta_r(y)$ are one of the above two types. We have also presented some conjectures on 3-valued and 5-valued $\Delta_r(y)$ that are not covered by the known theorems.

APPENDIX A

CROSS-CORRELATION VALUES

In APPENDIX A Δ_r and $\eta(\Delta_r)$ for all r are tabulated for $3 \leq n \leq 12$. For n = 13, 14 and 15, Δ_r and $\eta(\Delta_r)$ are given if $\Delta_r(y)$ is 7-valued or less. For n = 16, Δ_r and $\eta(\Delta_r)$ are given if $\Delta_r(y)$ is 5-valued or less. Δ_r and $\eta(\Delta_r)$ for $r = 2^{n-1}-1$ are also given for $13 \leq n \leq 16$.

Suppose we have 2 proper cyclotomic coset leaders r and q such that $r \cdot q \equiv 2^k \mod 2^n-1$. Then, in view of Lemma 2-3, Δ_r and $\eta(\Delta_r)$ are given provided $r \leq q$. See APPENDIX B for the inverse pair relation of cyclotomic coset leaders.

In APPENDIX A the first column is the cyclotomic coset leader r. The second column gives the number of distinct values that $\Delta_r(y)$ takes on. The numbers to the right give the distribution. $\eta(\Delta_r)$ and Δ_r are given in pair: the first number is $\eta(\Delta_r)$ and the second number in parentheses is Δ_r.

EXAMPLE: For n = 7, $\Delta_9(y)$ is 3-valued. $\Delta_9(y) = 16$ 36 times, $\Delta_9(y) = 0$ 64 times and $\Delta_9(y) = -16$ 28 times as y ranges over $GF(2^7)$. Note that $9 \cdot 15 = 135 \equiv 2^3 \mod 127$. The cyclotomic cosets containing 9 and 15 are inverse of each other, and $\Delta_9(y)$ is given but $\Delta_{15}(y)$ is omitted.

CROSS-CORRELATION OF MAXIMAL SEQUENCES

DEGREE 3

3	3	1(	4)	4(	0)	1(	-4)

DEGREE 4

7	4	2(	8)	4(	4)	4(	0)	4(	-4)

DEGREE 5

3	3	12(	8)	16(	0)	4(	-8)						
5	3	12(	8)	16(	0)	4(	-8)						
15	4	1(	12)	5(	8)	10(	4)	4(	0)	5(	-4)	5(	-8)

DEGREE 6

9	3	12(	16)	48(	0)	6(	-16)								
11	5	2(	24)	4(	16)	12(	8)	28(	0)	18(	-8)				
31	6	3(	16)	8(	12)	9(	8)	6(	4)	13(	0)	12(	-4)	7(	-8)	6(-12)

DEGREE 7

3	3	48(	16)	64(	0)	28(	-16)								
5	3	36(	16)	64(	0)	28(	-16)								
7	7	7(	24)	14(	16)	28(	8)	36(	0)	28(	-8)	14(	-16)	1(	-60)
9	3	36(	16)	64(	0)	28(	-16)								
11	3	36(	16)	64(	0)	28(	-16)								
17	7	7(	24)	14(	16)	28(	8)	36(	0)	28(	-8)	14(	-16)	1(	-60)
21	7	7(	24)	14(	16)	28(	8)	36(	0)	28(	-8)	14(	-16)	1(	-60)
23	3	36(	16)	64(	0)	28(	-16)								

61	11	7(29) 7(-29)		14(16)		14(12)		7(8)		21(4)		15(0)		7(-4)		21(-8)		8(-12)		7(-16)	

DEGREE 8

7	6	1(64)		14(32)		68(16)		105(0)		52(-16)		14(-32)									
11	7	4(48)		10(32)		68(16)		101(0)		64(-16)		8(-32)		1(-64)							
13	6	1(64)		4(48)		84(16)		101(0)		68(-16)		18(-32)									
19	5	8(48)		8(32)		64(16)		88(0)		88(-16)											
23	5	2(64)		20(32)		56(16)		90(0)		88(-16)											
31	6	60(32)		16(16)		120(0)		80(-16)													
43	6	2(96)		1(64)		76(16)		109(0)		60(-16)		8(-32)									
53	6	4(64)		24(16)		60(0)		96(-16)													
127	16	5(32) 14(-9)		8(28) 24(-12)		20(24) 18(-16)		16(20) 8(-20)		16(16) 16(-24)		16(12) 8(-28)		20(8)		16(4)		17(0)		32(-4)	

DEGREE 9

3	3	136(32)		256(0)		120(-32)															
5	3	136(32)		256(0)		120(-32)															
9	3	34(64)		464(0)		28(-64)															
11	5	9(64)		108(32)		296(0)		108(-32)		1(-64)											
13	3	136(32)		256(0)		120(-32)															
15	14	9(64) 14(-24)		9(48) 34(-32)		18(40) 27(-40)		18(32) 3(-48)		39(24)		45(16)		100(8)		73(0)		54(-8)		63(-16)	
17	3	136(32)		256(0)		120(-32)															
19	3	136(32)		256(0)		120(-32)															
23	5	9(64)		108(32)		286(0)		108(-32)		1(-64)											
29	8	1(80)		27(48)		54(32)		99(16)		148(0)		117(-16)		54(-32)		12(-48)					
37	9	3(96)		1(80)		9(64)		21(48)		27(32)		99(16)		163(0)		135(-16)		54(-32)			
39	8	30(48)		54(32)		99(16)		145(0)		108(-16)		72(-32)		3(-48)		1(-64)					

41	9	9(	64)	9(	64)	45(	32)	138(	16)	139(	0)	99(	-16)	63(	-32)	9(	-48)	1(	-112)		
43	5	9(	64)	129(	32)	286(	0)	108(	-32)	1(	-64)										
45	7	27(	64)	37(	42)	138(	16)	154(	0)	63(	-16)	81(	-32)	12(	-48)						
47	3	136(	32)	256(	0)	120(	-32)														
51	13	18(	48)	27(	48)	9(	32)	27(	24)	36(	16)	82(	8)	82(	0)	81(	-8)	54(	-16)	27(	-24)
		45(	-32)	9(	-48)	3(	-72)														
55	14	1(	104)	3(	44)	21(	48)	27(	40)	9(	32)	27(	24)	36(	16)	72(	8)	100(	0)	72(	-8)
		63(	-16)	36(	-24)	27(	-32)	18(	-40)												
61	8	27(	48)	54(	32)	102(	16)	148(	0)	117(	-16)	54(	-32)	9(	-48)	1(	-112)				
75	9	3(	96)	3(	64)	19(	48)	55(	32)	108(	16)	109(	0)	162(	-16)	54(	-32)				
79	8	1(	97)	27(	49)	54(	32)	99(	16)	148(	0)	117(	-16)	54(	-32)	12(	-48)				
93	9	3(	64)	9(	48)	81(	32)	108(	16)	109(	0)	135(	-16)	63(	-32)	3(	-48)	1(	-112)		
95	12	13(	56)	9(	48)	27(	32)	36(	24)	72(	16)	64(	8)	58(	0)	90(	-8)	45(	-16)	48(	-24)
		27(	-32)	18(	-48)																
139	5	9(	64)	129(	32)	286(	0)	104(	-32)	1(	-64)										
255	23	9(	64)	18(	40)	9(	36)	3(	32)	45(	28)	21(	24)	18(	20)	45(	16)	18(	12)	27(	8)
		45(	4)	19(	0)	19(	-4)	36(	-8)	27(	-12)	27(	-16)	27(	-20)	9(	-24)	18(	-28)	36(	-32)
		18(	-36)	9(	-40)	3(	-44)														

DEGREE 10

5	3	136(	64)	256(	0)	120(	-64)														
7	13	5(	96)	2(	80)	40(	64)	70(	48)	115(	32)	200(	16)	196(	0)	160(	-16)	135(	-32)	70(	-48)
		20(	-64)	10(	-80)	1(	-96)														
13	3	136(	64)	768(	0)	120(	-64)														
17	3	136(	64)	768(	0)	120(	-64)														
19	6	10(	96)	46(	64)	260(	32)	428(	0)	210(	-32)	70(	-64)								
23	11	7(	80)	55(	64)	50(	48)	130(	32)	175(	16)	171(	0)	246(	-16)	100(	-32)	40(	-48)	40(	-64)
		10(	-80)																		
25	3	136(	64)	764(	0)	120(	-64)														
29	11	3(	144)	15(	64)	125(	48)	150(	32)	135(	16)	173(	0)	155(	-16)	180(	-32)	70(	-48)	10(	-64)
		10(	-80)																		
35	5	40(	96)	16(	64)	240(	32)	368(	0)	360(	-32)										

37	7	10(96)	54(64)	240(32)	414(0)	260(-32)	40(-64)	2(-160)													
43	6	74(64)	250(32)	368(0)	300(-32)	20(-64)	10(-96)														
47	6	5(128)	10(96)	86(64)	160(32)	413(0)	350(-32)														
49	3	136(64)	76(0)	120(-64)																	
53	14	5(160)	10(96)	10(80)	25(64)	50(48)	110(32)	180(16)	186(0)	220(-16)	170(-32)										
		50(-48)	5(-64)	2(-80)	1(-96)																
59	12	10(96)	10(80)	11(64)	60(48)	135(32)	240(16)	183(0)	110(-16)	175(-32)	50(-48)										
		30(-64)	10(-80)																		
61	10	7(90)	35(64)	100(48)	120(32)	115(16)	231(0)	206(-16)	100(-32)	100(-48)	10(-96)										
71	11	5(96)	40(64)	80(48)	105(32)	190(16)	224(0)	140(-16)	125(-32)	70(-48)	40(-64)										
		1(-96)																			
73	13	5(96)	10(80)	30(64)	50(48)	135(32)	220(16)	196(0)	140(-16)	115(-32)	90(-48)										
		30(-64)	2(-80)	1(-96)																	
99	10	5(112)	10(80)	30(64)	100(48)	280(16)	196(0)	281(-16)	70(-48)	30(-64)	22(-80)										
91	12	5(96)	2(80)	40(64)	75(48)	115(32)	180(16)	196(0)	191(-16)	130(-32)	60(-48)										
		10(-64)	20(-80)																		
101	5	30(96)	56(64)	180(32)	408(0)	350(-32)															
103	11	50(64)	90(48)	115(32)	150(16)	188(0)	200(-16)	160(-32)	30(-48)	30(-64)	10(-80)										
		1(-96)																			
115	6	74(64)	250(32)	368(0)	300(-32)	20(-64)	10(-96)														
125	6	5(128)	10(96)	86(64)	160(32)	413(0)	350(-32)														
147	12	10(112)	2(64)	60(48)	145(32)	183(16)	236(0)	190(-16)	70(-32)	60(-48)	40(-64)										
		12(-80)	1(-96)																		
173	20	1(144)	10(72)	25(64)	10(56)	45(48)	70(40)	70(32)	70(24)	65(16)	90(8)										
		91(0)	120(-8)	175(-16)	50(-24)	40(-32)	62(-40)	20(-48)	20(-56)	30(-64)	10(-72)										
179	20	1(144)	5(112)	10(72)	30(56)	45(48)	40(40)	55(32)	90(24)	95(16)	110(8)										
		144(0)	70(-8)	80(-16)	60(-24)	35(-32)	62(-40)	30(-48)	20(-56)	20(-64)	20(-72)										
224	11	10(80)	41(64)	70(48)	105(32)	210(16)	193(0)	140(-16)	175(-32)	40(-48)	30(-64)										
		10(-80)																			
235	12	12(90)	90(64)	40(48)	115(32)	230(16)	186(0)	150(-16)	140(-32)	70(-48)	20(-64)										
		10(-80)	1(-96)																		
363	6	1(384)	2(320)	40(64)	220(32)	461(0)	300(-32)														
511	32	5(64)	20(60)	30(56)	20(52)	20(48)	20(44)	35(40)	50(36)	40(32)	20(28)										
		20(24)	50(20)	45(16)	50(12)	40(8)	30(4)	61(0)	40(-4)	20(-8)	40(-12)										
		45(-16)	20(-20)	40(-24)	40(-28)	20(-32)	40(-36)	40(-40)	30(-44)	20(-48)	30(-52)										
		11(-56)	12(-60)																		

DEGREE 11

3	3	528(	64)	1024(	0)	496(	-64)														
5	3	528(	64)	1024(	0)	496(	-64)														
7	9	11(	128)	77(	96)	176(	64)	517(	32)	562(	0)	407(	-32)	232(	-64)	55(	-96)	11(-128)			
9	3	528(	64)	1024(	0)	496(	-64)														
11	5	22(	128)	440(	64)	1156(	0)	408(	-64)	22(-128)											
13	3	528(	64)	1024(	0)	496(	-64)														
15	9	11(	128)	66(	96)	220(	64)	462(	32)	562(	0)	462(	-32)	188(	-64)	66(	-96)	11(-128)			
17	3	528(	64)	1024(	0)	496(	-64)														
19	10	1(	288)	11(	128)	44(	96)	220(	64)	517(	32)	562(	0)	396(	-32)	220(	-64)	66(	-96)	11(-128)	
21	9	11(	128)	44(	96)	231(	64)	418(	32)	617(	0)	462(	-32)	133(	-64)	110(	-96)				
23	5	22(	128)	440(	64)	1156(	0)	408(	-64)	22(-128)											
27	10	1(	288)	11(	128)	66(	96)	187(	64)	473(	32)	639(	0)	418(	-32)	165(	-64)	66(	-96)	22(-128)	
29	8	11(	128)	55(	96)	231(	64)	495(	32)	529(	0)	429(	-32)	221(	-64)	77(	-96)				
31	27	11(	120)	22(	104)	22(	88)	55(	80)	55(	72)	77(	64)	33(	56)	88(	48)	88(	40)	121(	32)
		122(	24)	44(	16)	176(	8)	188(	0)	187(	-8)	154(	-16)	99(	-24)	77(	-32)	66(	-40)	132(	-48)
		55(	-56)	33(	-64)	44(	-72)	44(	-80)	33(	-88)	11(	-112)	11(	-136)						
33	3	528(	64)	1024(	0)	496(	-64)														
35	3	528(	64)	1024(	0)	496(	-64)														
37	5	22(	128)	440(	64)	1156(	0)	408(	-64)	22(-128)											
39	10	1(	288)	11(	128)	44(	96)	242(	64)	451(	32)	606(	0)	440(	-32)	154(	-64)	88(	-96)	11(-128)	
41	10	1(	288)	11(	128)	44(	96)	220(	64)	517(	32)	562(	0)	396(	-32)	220(	-64)	66(	-96)	11(-128)	
43	3	528(	64)	1024(	0)	496(	-64)														
45	9	1(	288)	77(	96)	209(	64)	462(	32)	617(	0)	407(	-32)	187(	-64)	77(	-96)	11(-128)			
47	5	22(	128)	440(	64)	1156(	0)	408(	-64)	22(-128)											
51	9	11(	128)	77(	96)	176(	64)	517(	32)	562(	0)	407(	-32)	232(	-64)	55(	-96)	11(-128)			
53	8	99(	96)	198(	64)	451(	32)	562(	0)	473(	-32)	210(	-64)	33(	-96)	22(-128)					
55	9	11(	128)	66(	96)	220(	64)	462(	32)	562(	0)	462(	-32)	188(	-64)	66(	-96)	11(-128)			

97	3	5248	64)	10248	0)	4968	-64)														
99	10	1(	288)	22(	128)	55(	96)	143(	64)	528(	32)	683(	0)	341(	-32)	165(	-64)	99(	-96)	11(	-128
81	17	11(	128)	44(	96)	88(	80)	132(	64)	88(	48)	242(	32)	264(	16)	254(	0)	374(	-16)	220(	-32
		132(	-48)	99(	-64)	66(	-80)	22(	-96)	11(	-112)	11(	-128)	1(	-240)						
87	9	11(	128)	77(	96)	176(	64)	517(	32)	562(	0)	407(	-32)	232(	-64)	55(	-96)	11(	-128)		
71	9	11(	128)	55(	96)	264(	64)	407(	32)	562(	0)	517(	-32)	144(	-64)	77(	-96)	11(	-128)		
73	9	110(	96)	145(	64)	462(	32)	617(	0)	418(	-32)	199(	-64)	66(	-96)	11(	-128)				
75	8	11(	128)	44(	96)	253(	64)	506(	32)	485(	0)	440(	-32)	243(	-64)	66(	-96)				
81	5	22(	128)	440(	64)	1156(	0)	408(	-64)	22(	-128)										
93	14	1(	288)	11(	128)	33(	96)	55(	80)	99(	64)	198(	48)	242(	32)	286(	16)	287(	0)	275(	-16)
		187(	-32)	176(	-48)	55(	-64)	55(	-80)	77(	-96)	11(	-112)								
95	3	5248	64)	10248	0)	4968	-64)														
101	15	12(	112)	55(	96)	55(	80)	121(	64)	187(	48)	154(	32)	308(	16)	298(	0)	242(	-16)	275(	-32)
		143(	-48)	77(	-64)	55(	-80)	44(	-96)	22(	-12)										
103	9	11(	128)	66(	96)	220(	64)	462(	32)	562(	0)	462(	-32)	188(	-64)	66(	-96)	11(	-128)		
107	3	5248	64)	10248	0)	4968	-64)														
109	8	77(	96)	253(	64)	429(	32)	529(	0)	495(	-32)	199(	-64)	55(	-96)	11(	-128)				
111	15	12(	112)	33(	96)	99(	80)	99(	64)	198(	48)	198(	32)	264(	16)	265(	0)	275(	-16)	286(	-32)
		132(	-48)	77(	-64)	55(	-80)	55(	-96)	11(	-112)										
113	9	11(	128)	77(	96)	165(	64)	539(	32)	573(	0)	363(	-32)	243(	-64)	77(	-96)				
115	17	11(	144)	11(	128)	11(	112)	88(	80)	99(	64)	110(	48)	286(	32)	308(	16)	276(	0)	286(	-16)
		241(	-32)	121(	-48)	66(	-64)	77(	-80)	55(	-96)	11(	-112)	1(	-240)						
121	5	22(	128)	440(	64)	1156(	0)	408(	-64)	22(	-128)										
123	9	11(	128)	88(	96)	198(	64)	396(	32)	628(	0)	528(	-32)	122(	-64)	44(	-96)	33(	-128)		
125	14	11(	128)	12(	112)	33(	96)	44(	80)	121(	64)	165(	48)	253(	32)	219(	16)	221(	0)	286(	-16)
		187(	-32)	154(	-48)	143(	-64)	33(	-80)	55(	-96)	11(	-112)								
127	16	11(	128)	23(	112)	22(	96)	44(	80)	88(	64)	209(	48)	275(	32)	242(	16)	276(	0)	275(	-16)
		198(	-32)	154(	-48)	110(	-64)	77(	-80)	33(	-96)	11(	-128)								
141	5	33(	128)	396(	64)	1222(	0)	364(	-64)	33(	-128)										
147	9	11(	128)	77(	96)	209(	64)	440(	32)	573(	0)	484(	-32)	199(	-64)	44(	-96)	11(	-160)		
149	16	22(	128)	23(	112)	77(	80)	55(	64)	176(	48)	286(	32)	264(	16)	331(	0)	231(	-16)	220(	-32
		165(	-48)	77(	-64)	66(	-80)	22(	-96)	22(	-112)	11(	-128)								
155	15	22(	112)	33(	96)	88(	80)	121(	64)	121(	48)	199(	32)	264(	16)	331(	0)	341(	-16)	176(	-32)

		1424	-64)	1004	-44)	77(	-80)	33(	-96)	11(-144)											
157	7	1104	96)	154(	64)	484(	32)	628(	0)	374(	-32)	210(	-64)	88(	-96)						
163	9	22(	128)	55(	96)	209(	64)	451(	32)	573(	0)	517(	-32)	155(	-64)	33(	-96)	33(-128)			
165	9	11(	128)	77(	96)	198(	64)	451(	32)	604(	0)	451(	-32)	166(	-64)	77(	-96)	11(-128)			
167	15	231	112)	44(	96)	66(	80)	88(	64)	132(	48)	264(	32)	319(	16)	276(	0)	275(	-16)	176(	-32)
		132(	-44)	132(	-64)	44(	-80)	44(	-96)	11(-112)											
169	9	22(	128)	55(	96)	209(	64)	418(	32)	694(	0)	363(	-32)	221(	-64)	44(	-96)	22(-128)			
171	5	22(	124)	440(	64)	1156(	0)	404(	-64)	22(-128)											
175	17	22(	128)	11(	112)	44(	96)	33(	80)	66(	64)	231(	48)	253(	32)	297(	16)	264(	0)	231(	-16)
		198(	-32)	187(	-48)	132(	-64)	33(	-80)	33(	-96)	11(-112)		11(-128)							
177	15	231	112)	33(	96)	44(	80)	110(	64)	242(	48)	220(	32)	220(	16)	297(	0)	242(	-16)	220(	-32)
		187(	-48)	143(	-64)	33(	-80)	11(	-96)	33(-112)											
181	9	231	128)	22(	96)	198(	64)	550(	32)	540(	0)	418(	-32)	210(	-64)	66(	-96)	11(-128)			
185	16	11(	128)	11(	112)	33(	96)	88(	80)	99(	64)	154(	48)	275(	32)	231(	16)	264(	0)	286(	-16)
		242(	-32)	143(	-48)	66(	-64)	99(	-80)	22(	-96)	22(-112)									
187	5	22(	128)	440(	64)	1156(	0)	408(	-64)	22(-128)											
191	9	33(	128)	33(	96)	165(	64)	561(	32)	595(	0)	363(	-32)	199(	-64)	99(	-96)				
199	29	11(	144)	22(	112)	11(	104)	22(	88)	33(	80)	44(	72)	22(	64)	55(	56)	66(	48)	88(	40)
		176(	32)	177(	24)	143(	16)	176(	8)	100(	0)	110(	-8)	165(	-16)	121(	-24)	88(	-32)	99(	-40)
		55(	-48)	55(	-56)	77(	-64)	33(	-72)	33(	-80)	22(	-88)	22(	-96)	11(-120)		11(-128)			
215	9	11(	124)	66(	96)	209(	64)	484(	32)	573(	0)	418(	-32)	199(	-64)	88(	-96)				
217	9	11(	128)	99(	96)	187(	64)	418(	32)	639(	0)	484(	-32)	133(	-64)	66(	-96)	22(-128)			
221	5	22(	124)	440(	64)	1156(	0)	408(	-64)	22(-128)											
229	5	22(	128)	440(	64)	1156(	0)	404(	-64)	22(-128)											
235	5	22(	128)	440(	64)	1156(	0)	404(	-64)	22(-128)											
245	17	11(	176)	33(	112)	22(	80)	110(	64)	176(	48)	275(	32)	308(	16)	298(	0)	242(	-16)	220(	-32)
		154(	-48)	88(	-64)	55(	-80)	33(	-96)	11(-112)		11(-144)		1(-240)							
247	9	22(	128)	44(	96)	198(	64)	528(	32)	562(	0)	396(	-32)	210(	-64)	88(	-96)				
251	9	22(	128)	33(	96)	242(	64)	462(	32)	617(	0)	341(	-32)	276(	-64)	44(	-96)	11(-128)			
255	16	11(	144)	11(	112)	33(	96)	55(	80)	121(	64)	198(	48)	209(	32)	275(	16)	331(	0)	231(	-16)
		165(	-32)	187(	-48)	121(	-64)	66(	-80)	33(	-96)	11(-128)									
271	29	11(	128)	11(	112)	11(	96)	44(	88)	33(	80)	66(	72)	22(	64)	44(	56)	66(	48)	132(	40)
		99(	32)	144(	24)	143(	16)	154(	8)	210(	0)	77(	-8)	187(	-16)	77(	-24)	66(	-32)	110(	-40)
		66(	-48)	66(	-56)	44(	-64)	77(	-72)	22(	-80)	33(	-88)	22(	-96)	11(-128)					

307	29	11(128)	11(120)	11(112)	11(104)	11(88)	11(80)	44(72)	66(64)	66(56)	88(48)										
		165(40)	110(32)	100(24)	143(16)	110(8)	144(0)	176(-8)	143(-16)	110(-24)	110(-32)										
		77(-40)	88(-48)	44(-56)	33(-64)	33(-72)	44(-80)	44(-88)	22(-96)	22(-104)											
311	5	22(128)	440(64)	1156(0)	408(-64)	22(-128)															
317	8	77(96)	253(64)	429(32)	529(0)	495(-32)	199(-64)	55(-96)	11(-128)												
319	9	11(128)	66(96)	220(64)	462(32)	562(0)	462(-32)	188(-64)	66(-96)	11(-128)											
333	8	11(128)	66(96)	209(64)	484(32)	573(0)	418(-32)	199(-64)	88(-96)												
341	29	11(128)	11(112)	11(104)	33(88)	55(80)	33(72)	33(64)	44(56)	99(48)	132(40)										
		88(32)	132(24)	154(16)	132(8)	155(0)	187(-8)	99(-16)	110(-24)	121(-32)	77(-40)										
		66(-48)	77(-56)	55(-64)	11(-72)	33(-80)	33(-88)	33(-96)	11(-104)	11(-112)											
347	9	11(128)	66(96)	220(64)	462(32)	562(0)	462(-32)	188(-64)	66(-96)	11(-128)											
353	9	11(128)	55(96)	286(64)	330(32)	661(0)	451(-32)	188(-64)	44(-96)	22(-128)											
371	16	11(160)	1(112)	11(96)	0(80)	99(64)	198(48)	231(32)	264(16)	320(0)	231(-16)										
		231(-32)	154(-48)	77(-64)	66(-80)	44(-96)	22(-112)														
415	9	22(128)	33(96)	231(64)	517(32)	507(0)	451(-32)	221(-64)	55(-96)	11(-128)											
443	16	11(128)	12(112)	22(96)	88(80)	99(64)	132(48)	242(32)	330(16)	298(0)	198(-16)										
		220(-32)	198(-48)	77(-64)	66(-80)	44(-96)	11(-128)														
463	15	11(128)	12(112)	22(96)	66(80)	132(64)	165(48)	185(32)	330(16)	353(0)	220(-16)										
		198(-32)	132(-48)	88(-64)	99(-80)	55(-96)															
477	16	11(128)	1(112)	33(96)	66(80)	121(64)	187(48)	220(32)	297(16)	243(0)	253(-16)										
		231(-32)	154(-48)	121(-64)	55(-80)	44(-96)	11(-112)														
491	15	23(112)	22(96)	66(80)	143(64)	165(48)	220(32)	231(16)	298(0)	341(-16)	154(-32)										
		132(-48)	143(-64)	55(-80)	44(-96)	11(-112)															
497	16	11(128)	12(112)	33(96)	55(80)	99(64)	209(48)	220(32)	242(16)	287(0)	308(-16)										
		231(-32)	121(-48)	99(-64)	55(-80)	44(-96)	22(-112)														
1023	45	22(84)	11(86)	33(80)	44(76)	22(72)	23(68)	44(64)	44(60)	33(56)	99(52)										
		44(48)	33(44)	88(40)	33(36)	44(32)	66(28)	44(24)	66(20)	44(16)	66(12)										
		22(8)	77(4)	56(0)	33(-4)	121(-8)	22(-12)	44(-16)	110(-20)	44(-24)	33(-28)										
		77(-32)	33(-36)	44(-40)	66(-44)	33(-48)	22(-52)	55(-56)	44(-60)	33(-64)	66(-68)										
		22(-72)	22(-76)	44(-80)	11(-84)	11(-88)															

DEGREE 12

11	7	1(384)	24(192)	193(128)	1109(64)	1490(0)	1052(-64)	228(-128)													
17	3	136(256)	3840(0)	120(-256)																	
19	8	1(256)	24(192)	282(128)	864(64)	1689(0)	1044(-64)	180(-128)	12(-192)												

23	13	7(256)	12(224)	48(160)	141(128)	224(96)	456(64)	672(32)	877(0)	804(-32)	444(-64)	
		244(-96)	111(-128)	12(-192)								
29	13	60(192)	60(160)	71(128)	216(96)	440(64)	724(32)	878(0)	808(-32)	480(-64)	180(-96)	
		72(-128)	48(-160)	12(-224)								
31	23	6(192)	24(176)	24(160)	36(144)	69(128)	120(112)	124(96)	186(80)	216(64)	256(48)	
		252(32)	462(16)	461(0)	402(-16)	388(-32)	292(-48)	264(-64)	252(-80)	120(-96)	48(-112)	
		24(-128)	36(-144)	36(-160)								
37	14	3(256)	24(192)	28(160)	136(128)	288(96)	372(64)	712(32)	939(0)	720(-32)	516(-64)	
		252(-96)	36(-128)	48(-160)	24(-192)							
41	7	9(256)	72(192)	176(128)	892(64)	1453(0)	1156(-64)	138(-128)				
43	7	1(384)	24(192)	193(128)	1109(64)	1490(0)	1052(-64)	228(-128)				
47	25	12(288)	3(192)	12(176)	24(160)	52(144)	96(128)	66(112)	102(96)	138(80)	216(64)	
		33(48)	318(32)	462(16)	485(0)	342(-16)	339(-32)	340(-48)	240(-64)	204(-80)	120(-96)	
		54(-112)	48(-128)	24(-144)	24(-160)	1(-224)						
53	12	2(384)	7(256)	48(160)	108(128)	268(96)	528(64)	684(32)	791(0)	708(-32)	504(-64)	
		360(-96)	108(-128)									
59	23	1(288)	4(256)	20(176)	34(144)	78(128)	114(112)	129(96)	162(80)	231(64)	288(48)	
		384(32)	342(16)	462(0)	486(-16)	276(-32)	340(-48)	222(-64)	168(-80)	132(-96)	120(-112)	
		36(-128)	48(-144)	4(-160)								
61	25	2(336)	6(224)	15(192)	6(176)	27(160)	36(144)	18(128)	72(112)	120(96)	264(80)	
		264(64)	264(48)	372(32)	456(16)	401(0)	282(-16)	295(-32)	398(-48)	258(-64)	192(-80)	
		192(-96)	96(-112)	36(-128)	12(-144)	24(-160)						
67	5	160(192)	32(128)	1024(64)	1376(0)	1504(-64)						
71	6	211(256)	44(192)	272(128)	772(64)	1509(0)	1476(-64)					
73	5	336(128)	768(64)	1920(0)	768(-64)	904(-128)						
79	7	12(320)	7(256)	64(192)	234(128)	744(64)	1607(0)	1428(-64)				
83	24	6(192)	12(176)	48(160)	12(144)	87(128)	132(112)	110(96)	168(80)	192(64)	256(48)	
		372(32)	432(16)	413(0)	396(-16)	294(-32)	340(-48)	345(-64)	204(-80)	144(-96)	60(-112)	
		12(-128)	24(-144)	24(-160)	12(-176)							
89	15	2(320)	30(192)	36(160)	105(128)	156(96)	569(64)	804(32)	812(0)	708(-32)	484(-64)	
		264(-96)	99(-128)	24(-160)	12(-192)	12(-224)						
97	7	12(256)	272(128)	832(64)	1896(0)	832(-64)	240(-128)	12(-256)				
101	15	2(320)	6(256)	4(192)	12(160)	117(128)	288(96)	540(64)	756(32)	818(0)	624(-32)	
		528(-64)	312(-96)	91(-128)	12(-160)	24(-192)						
103	13	2(256)	12(224)	60(160)	102(128)	288(96)	468(64)	684(32)	895(0)	696(-32)	516(-64)	
		312(-96)	60(-128)	36(-160)								
109	6	42(192)	225(128)	986(64)	1518(0)	1158(-64)	169(-128)					

121	14	1(256) 544(-64)	12(224) 324(-96)	13(192) 60(-128)	60(160) 24(-160)	54(128)	272(96)	564(64)	624(32)	805(0)	732(-32)
127	4	672(128)	64(64)	2016(0)	1344(-64)						
137	14	2(384) 864(-32)	8(288) 456(-64)	7(256) 312(-96)	4(192) 72(-128)	72(160)	108(128)	288(96)	396(64)	504(32)	1003(0)
139	14	1(256) 312(-96)	22(192) 97(-128)	36(160) 12(-160)	117(128) 4(-192)	268(96)	486(64)	684(32)	855(0)	672(-32)	528(-64)
149	8	1(384)	3(192)	209(128)	1024(64)	1586(0)	1058(-64)	168(-128)	24(-192)		
151	13	1(256) 252(-96)	22(192) 75(-128)	36(160) 24(-160)	153(128)	288(96)	444(64)	576(32)	875(0)	744(-32)	606(-64)
157	29	4(240) 864(48) 84(-112)	4(208) 234(32) 24(-128)	3(192) 312(16) 48(-144)	12(160) 451(0) 24(-192)	6(144) 490(-16) 2(-208)	78(128) 442(-32)	138(112) 192(-48)	171(96) 216(-64)	180(80) 252(-80)	180(64) 121(-96)
163	13	12(192) 51(-128)	36(160) 24(-160)	135(128) 12(-192)	300(96)	460(64)	636(32)	942(0)	588(-32)	564(-64)	336(-96)
167	13	24(192) 51(-128)	48(160) 12(-160)	153(128) 24(-192)	272(96)	288(64)	804(32)	834(0)	852(-32)	408(-64)	316(-96)
173	23	15(224) 408(32) 24(-128)	4(192) 320(16) 36(-144)	13(160) 331(0) 12(-160)	52(144) 396(-16)	12(128) 330(-32)	132(112) 336(-48)	186(96) 288(-64)	144(80) 204(-80)	219(64) 172(-96)	308(48) 84(-112)
181	24	4(288) 264(64) 102(-96)	4(256) 320(48) 48(-112)	15(192) 372(32) 120(-128)	24(176) 360(16) 88(-144)	1(160) 415(0)	6(144) 456(-16)	24(128) 432(-32)	150(112) 216(-48)	129(96) 132(-64)	150(80) 312(-80)
187	22	1(288) 372(16) 60(-144)	12(192) 432(0) 12(-192)	30(144) 336(-16)	66(128) 387(-32)	114(112) 348(-48)	150(96) 210(-64)	250(80) 204(-80)	216(64) 156(-96)	304(48) 84(-112)	330(32) 28(-128)
197	7	12(320)	16(256)	40(192)	240(128)	780(64)	1568(0)	1440(-64)			
199	23	6(256) 444(48) 96(-112)	11(192) 264(32) 54(-128)	12(176) 349(16) 40(-144)	24(160) 397(0)	36(144) 552(-16)	27(128) 276(-32)	120(112) 264(-48)	156(96) 222(-64)	120(80) 252(-80)	211(64) 144(-96)
239	24	12(288) 408(48) 156(-112)	3(192) 372(32) 84(-128)	12(176) 312(16) 36(-144)	6(160) 425(0) 2(-160)	36(144) 390(-16) 12(-176)	51(128) 390(-32) 1(-192)	88(112) 312(-48)	84(96) 216(-64)	184(80) 180(-80)	324(64) 138(-96)
211	25	6(320) 312(48) 60(-112)	7(192) 414(32) 48(-128)	24(176) 384(16) 16(-144)	18(160) 469(0) 12(-160)	28(144) 348(-16) 12(-176)	75(128) 300(-32)	60(112) 324(-48)	116(96) 270(-64)	216(80) 264(-80)	181(64) 132(-96)
239	44	1(480) 48(128) 192(48) 144(-64) 44(-128)	6(288) 60(112) 114(32) 144(-64) 12(-128)	2(272) 84(104) 168(24) 180(-56) 12(-136)	4(248) 132(96) 132(16) 192(-64) 36(-144)	4(232) 72(88) 144(-8) 60(-72)	4(208) 78(80) 240(0) 72(-80)	15(192) 84(72) 324(-8) 120(-88)	12(152) 114(64) 240(-16) 33(-96)	12(144) 120(56) 180(-24) 36(-104)	18(128) 126(48) 180(-32) 48(-112)

251	27	1(288)	6(240)	3(224)	2(176)	12(160)	6(144)	132(128)	84(112)	78(96)	250(80)	
		216(64)	282(48)	342(32)	444(16)	468(0)	372(-16)	360(-32)	328(-48)	198(-64)	204(-80)	
		120(-96)	60(-112)	74(-128)	30(-144)	12(-160)	12(-176)	12(-192)				
293	5	33(256)	342(128)	724(64)	1521(0)	1476(-64)						
277	9	1(384)	6(320)	4(256)	22(192)	240(128)	906(64)	1648(0)	1098(-64)	171(-128)		
283	24	6(288)	24(176)	18(160)	48(144)	66(128)	48(112)	105(96)	126(80)	228(64)	456(48)	
		420(32)	282(16)	445(0)	478(-16)	376(-32)	276(-48)	135(-64)	228(-80)	108(-96)	48(-112)	
		90(-128)	60(-144)	12(-160)	12(-192)							
293	12	6(448)	3(512)	162(128)	288(96)	246(64)	864(32)	1079(0)	516(-32)	570(-64)	280(-96)	
		48(-128)	36(-160)									
307	26	3(224)	6(192)	12(176)	24(160)	58(144)	42(128)	36(112)	120(96)	238(80)	168(64)	
		480(48)	324(32)	456(16)	378(0)	456(-16)	124(-32)	462(-48)	276(-64)	216(-80)	72(-96)	
		136(-112)	54(-128)	12(-160)	12(-176)	12(-192)	1(-288)					
319	7	12(320)	1(256)	64(192)	234(128)	744(64)	1607(0)	1428(-64)				
331	8	2(384)	12(320)	7(256)	36(192)	276(128)	744(64)	1579(0)	1440(-64)			
361	13	1(192)	24(176)	40(144)	66(128)	72(112)	360(80)	264(64)	504(48)	616(16)	382(0)	
		480(-16)	420(-48)	252(-64)	336(-80)	184(-112)	48(-128)	24(-144)	12(-176)			
349	24	19(192)	12(176)	36(160)	36(144)	60(128)	72(112)	140(96)	132(80)	288(64)	252(48)	
		434(32)	384(16)	312(0)	408(-16)	354(-32)	364(-48)	285(-64)	228(-80)	100(-96)	84(-112)	
		48(-128)	12(-144)	12(-160)	12(-192)							
341	13	1(256)	48(192)	24(160)	129(128)	280(96)	420(64)	696(32)	807(0)	768(-32)	564(-64)	
		256(-96)	48(-128)	24(-160)								
347	13	4(256)	44(160)	80(128)	216(96)	570(64)	820(32)	744(0)	636(-32)	528(-64)	300(-96)	
		96(-128)	12(-160)	22(-192)								
377	7	12(320)	10(256)	52(192)	252(128)	732(64)	1610(0)	1428(-64)				
397	14	1(384)	6(256)	12(224)	12(192)	72(160)	131(128)	192(96)	396(64)	808(32)	652(0)	
		916(-32)	528(-64)	304(-96)	66(-128)							
409	22	4(288)	24(176)	48(160)	54(144)	39(128)	60(112)	96(96)	192(80)	144(64)	468(48)	
		276(32)	534(16)	343(0)	408(-16)	196(-32)	418(-48)	294(-64)	192(-80)	64(-96)	156(-112)	
		36(-128)	42(-144)									
431	23	2(224)	14(208)	12(160)	48(144)	78(128)	84(112)	108(96)	132(80)	315(64)	324(48)	
		336(32)	432(16)	398(0)	376(-16)	354(-32)	324(-48)	204(-64)	180(-80)	180(-96)	72(-112)	
		40(-128)	60(-144)	11(-192)								
433	23	1(736)	3(576)	3(544)	12(176)	16(144)	72(128)	24(112)	168(96)	186(80)	162(64)	
		450(48)	474(32)	270(16)	408(0)	426(-16)	270(-32)	408(-48)	294(-64)	102(-80)	212(-96)	
		84(-112)	12(-128)	38(-144)								
457	4	8(512)	1792(64)	504(0)	1792(-64)							
441	9	6(256)	4(192)	264(128)	916(64)	1760(0)	892(-64)	240(-128)	12(-192)	2(-256)		

463	9	8(512)	1(384)	2(320)	1414(64)	1586(0)	820(-64)	219(-128)	36(-192)	12(-256)			
467	13	4(256)	14(192)	48(160)	81(128)	340(96)	432(64)	624(32)	980(0)	648(-32)	474(-64)		
		352(-96)	48(-128)	36(-160)									
479	13	18(192)	42(160)	120(128)	228(96)	504(64)	748(32)	870(0)	684(-32)	438(-64)	300(-96)		
		96(-128)	48(-160)	2(-256)									
491	13	12(192)	48(160)	164(128)	192(96)	448(64)	732(32)	900(0)	708(-32)	534(-64)	228(-96)		
		96(-128)	24(-160)	24(-192)									
497	24	2(640)	9(256)	12(192)	24(176)	78(160)	24(144)	78(128)	108(112)	60(96)	132(80)		
		144(64)	304(48)	258(32)	312(16)	491(0)	468(-16)	570(-32)	412(-48)	180(-64)	216(-80)		
		108(-96)	48(-112)	42(-128)	12(-160)								
599	24	3(640)	3(576)	1(448)	12(176)	40(144)	96(128)	36(112)	138(96)	192(80)	90(64)		
		384(48)	444(32)	300(16)	564(0)	456(-16)	246(-32)	408(-48)	258(-64)	144(-80)	152(-96)		
		84(-112)	36(-128)	12(-144)	12(-160)								
617	24	3(320)	12(224)	42(160)	24(144)	36(128)	120(112)	132(96)	192(80)	277(64)	284(48)		
		264(32)	312(16)	402(0)	564(-416)	378(-32)	340(-48)	282(-64)	156(-80)	120(-96)	84(-112)		
		24(-128)	12(-144)	12(-160)	24(-208)								
671	13	1(384)	24(160)	131(128)	388(96)	378(64)	648(32)	916(0)	748(-32)	450(-64)	264(-96)		
		96(-128)	40(-160)	12(-192)									
683	6	1(1408)	2(1344)	1218(64)	1804(0)	924(-64)	147(-128)						
701	6	12(256)	44(192)	296(128)	688(64)	1590(0)	1456(-64)						
721	7	4(832)	1(768)	24(192)	242(128)	768(64)	1733(0)	1324(-64)					
727	7	1(1024)	4(768)	12(256)	244(128)	720(64)	1709(0)	1296(-64)					
829	13	7(256)	9(192)	60(160)	114(128)	228(96)	486(64)	720(32)	837(0)	732(-32)	522(-64)		
		228(-96)	138(-128)	24(-160)									
877	12	4(224)	12(192)	24(160)	191(128)	192(96)	408(64)	864(32)	846(0)	652(-32)	420(-64)		
		312(-96)	171(-128)										
997	13	1(256)	24(192)	72(160)	108(128)	184(96)	546(64)	564(32)	991(0)	768(-32)	462(-64)		
		228(-96)	108(-128)	48(-160)									
2247	44	12(128)	12(124)	30(120)	52(116)	24(112)	48(108)	60(104)	36(100)	72(96)	48(92)		
		48(88)	108(84)	81(80)	48(76)	72(72)	48(68)	48(64)	48(60)	96(56)	48(52)		
		112(48)	120(44)	48(40)	72(36)	48(32)	96(28)	48(24)	84(20)	96(16)	60(12)		
		104(8)	72(4)	73(0)	96(-4)	48(-8)	96(-12)	96(-16)	36(-20)	144(-24)	108(-28)		
		48(-32)	96(-36)	78(-40)	60(-44)	72(-48)	84(-52)	48(-56)	96(-60)	120(-64)	60(-68)		
		48(-72)	48(-76)	24(-80)	96(-84)	48(-88)	48(-92)	75(-96)	48(-100)	48(-104)	24(-108)		
		48(-112)	28(-116)	24(-120)	24(-124)								

DEGREE 13

3	3	20800	1280	40960	0)	20160	-1280)				
5	3	20800	1280	40960	0)	20160	-1280)				
9	3	20800	1280	40960	0)	20160	-1280)				
11	5	910	2560	17160	1280	46420	0)	16520	-1280)	910	-2560)
13	3	20800	1280	40960	0)	20160	-1280)				
17	3	20800	1280	40960	0)	20160	-1280)				
19	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)
33	3	20800	1280	40960	0)	20160	-1280)				
43	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)
57	3	20800	1280	40960	0)	20160	-1280)				
65	3	20800	1280	40960	0)	20160	-1280)				
67	3	20800	1280	40960	0)	20160	-1280)				
71	3	20800	1280	40960	0)	20160	-1280)				
95	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)
113	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)
147	5	650	2560	18200	1280)	44860	0)	17560	-1280)	650	-2560)
161	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)
171	3	20800	1280	40960	0)	20160	-1280)				
191	3	20800	1280	40960	0)	20160	-1280)				
205	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)
225	5	650	2560	18200	1280)	44860	0)	17560	-1280)	650	-2560)
287	3	20800	1280	40960	0)	20160	-1280)				
445	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)
483	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)
631	5	780	2560	17680	1280)	45640	0)	17040	-1280)	780	-2560)
683	5	910	2560	17160	1280)	46420	0)	16520	-1280)	910	-2560)

749	5	91(	256)	1716(	128)	4642(	0)	1652(	-128)	91(	-256)						
869	5	91(	256)	1716(	128)	4642(	0)	1652(	-128)	91(	-256)						
939	5	91(	256)	1716(	128)	4642(	0)	1652(	-128)	91(	-256)						
4095	91	13(	180)	13(	176)	65(	172)	52(	168)	39(	164)	65(	160)	26(	156)	39(	152)
		91(	148)	78(	144)	52(	140)	91(	136)	39(	132)	104(	128)	182(	124)	52(	120)
		65(	116)	104(	112)	91(	108)	65(	104)	156(	100)	65(	96)	52(	92)	182(	88)
		104(	84)	52(	80)	117(	76)	52(	72)	117(	68)	182(	64)	65(	60)	91(	56)
		130(	52)	91(	48)	117(	44)	169(	40)	65(	36)	104(	32)	208(	28)	104(	24)
		52(	20)	156(	16)	91(	12)	65(	8)	260(	4)	53(	0)	78(	-4)	143(	-8)
		104(	-12)	143(	-16)	117(	-20)	91(	-24)	52(	-28)	182(	-32)	78(	-36)	78(	-40)
		130(	-44)	65(	-48)	117(	-52)	234(	-56)	52(	-60)	52(	-64)	104(	-68)	130(	-72)
		91(	-76)	156(	-80)	52(	-84)	65(	-88)	208(	-92)	104(	-96)	91(	-100)	104(	-104)
		65(	-108)	52(	-112)	117(	-116)	39(	-120)	52(	-124)	91(	-128)	78(	-132)	91(	-136)
		117(	-140)	39(	-144)	39(	-148)	117(	-152)	52(	-156)	26(	-160)	78(	-164)	26(	-168)
		26(	-172)	39(	-176)	1(	-180)										

DEGREE 14

5	3	2080(	256)	12288(	0)	2016(	-256)										
13	3	2080(	256)	12288(	0)	2016(	-256)										
17	3	2080(	256)	12288(	0)	2016(	-256)										
35	7	84(	384)	904(	256)	3948(	128)	6576(	0)	3948(	-128)	840(	-256)	84(	-384)		
65	3	2080(	256)	12288(	0)	2016(	-256)										
113	3	2080(	256)	12288(	0)	2016(	-256)										
131	5	672(	384)	64(	256)	4032(	128)	5568(	0)	6048(	-128)						
133	7	224(	384)	736(	256)	3360(	128)	7808(	0)	3360(	-128)	672(	-256)	224(	-384)		
137	7	224(	384)	736(	256)	3360(	128)	7808(	0)	3360(	-128)	672(	-256)	224(	-384)		
143	7	14(	640)	14(	512)	350(	384)	932(	256)	3010(	128)	6142(	0)	5922(	-128)		
191	6	126(	512)	42(	384)	1324(	256)	2772(	128)	6198(	0)	5922(	-128)				
193	3	2080(	256)	12288(	0)	2016(	-256)										
205	3	2080(	256)	12288(	0)	2016(	-256)										
265	7	28(	384)	1100(	256)	3696(	128)	6744(	0)	3836(	-128)	924(	-256)	56(	-384)		
277	7	70(	384)	960(	256)	3878(	128)	6576(	0)	4018(	-128)	784(	-256)	98(	-384)		
319	3	2080(	256)	12288(	0)	2016(	-256)										
389	7	14(	640)	42(	512)	252(	384)	1044(	256)	2982(	128)	6114(	0)	5936(	-128)		

397	6	56(	512)	280(	384)	1072(	256)	2800(	128)	6296(	0)	5880(	-128)				
413	6	56(	512)	294(	384)	1016(	256)	2884(	128)	6240(	0)	5894(	-128)				
445	6	49(	512)	336(	384)	918(	256)	2996(	128)	6177(	0)	5908(	-128)				
509	6	126(	512)	42(	384)	1324(	256)	2772(	128)	6198(	0)	5922(	-128)				
539	7	56(	384)	1002(	256)	3822(	128)	6660(	0)	3892(	-128)	882(	-256)	70(	-384)		
583	7	42(	384)	960(	256)	4102(	128)	6240(	0)	4102(	-128)	896(	-256)	42(	-384)		
667	7	14(	640)	49(	512)	252(	384)	974(	256)	3122(	128)	6009(	0)	5964(	-128)		
683	7	42(	384)	974(	256)	4144(	128)	5932(	0)	4634(	-128)	518(	-256)	140(	-384)		
743	6	70(	512)	252(	384)	1044(	256)	2912(	128)	6198(	0)	5908(	-128)				
893	7	7(	768)	35(	512)	294(	384)	981(	256)	3052(	128)	6065(	0)	5950(	-128)		
905	7	14(	640)	42(	512)	266(	384)	988(	256)	3066(	128)	6058(	0)	5950(	-128)		
953	6	56(	512)	294(	384)	1016(	256)	2884(	128)	6240(	0)	5894(	-128)				
1147	7	14(	640)	21(	512)	322(	384)	974(	256)	2982(	128)	6149(	0)	5922(	-128)		
1163	7	84(	384)	874(	256)	4032(	128)	6520(	0)	3892(	-128)	924(	-256)	56(	-384)		
1175	6	70(	512)	266(	384)	988(	256)	2996(	128)	6142(	0)	5922(	-128)				
1271	6	42(	512)	336(	384)	988(	256)	2856(	128)	6282(	0)	5880(	-128)				
1529	7	14(	640)	49(	512)	238(	384)	1030(	256)	3038(	128)	6065(	0)	5950(	-128)		
1655	7	14(	640)	28(	512)	266(	384)	1128(	256)	2786(	128)	6268(	0)	5894(	-128)		
1835	7	42(	384)	974(	256)	4144(	128)	5932(	0)	4634(	-128)	518(	-256)	140(	-384)		
1937	6	49(	512)	322(	384)	974(	256)	2912(	128)	6233(	0)	5894(	-128)				
1939	6	56(	512)	308(	384)	960(	256)	2968(	128)	6184(	0)	5908(	-128)				
2483	7	42(	384)	974(	256)	4144(	128)	5932(	0)	4634(	-128)	518(	-256)	140(	-384)		
2731	6	1(	5632)	2(	5376)	616(	256)	3612(	128)	7309(	0)	4844(	-128)				
8191	128	14(	256)	30(	252)	63(	248)	42(	244)	84(	240)	84(	236)	49(	232)	56(	228)
		56(	224)	98(	220)	140(	216)	70(	212)	63(	208)	112(	204)	112(	200)	84(	196)
		112(	192)	112(	188)	56(	184)	112(	180)	189(	176)	112(	172)	140(	168)	84(	164)
		140(	160)	140(	156)	112(	152)	84(	148)	112(	144)	168(	140)	154(	136)	252(	132)
		112(	128)	84(	124)	168(	120)	224(	116)	84(	112)	154(	108)	140(	104)	112(	100)
		224(	96)	168(	92)	120(	88)	140(	84)	168(	80)	126(	76)	168(	72)	224(	68)
		84(	64)	140(	60)	168(	56)	112(	52)	168(	48)	112(	44)	112(	40)	168(	36)
		294(	32)	70(	28)	252(	24)	196(	20)	140(	16)	196(	12)	112(	8)	112(	4)
		112(	0)	350(	-4)	112(	-8)	182(	-12)	168(	-16)	140(	-20)	168(	-24)	112(	-28)
		112(	-32)	168(	-36)	224(	-40)	168(	-44)	140(	-48)	112(	-52)	84(	-56)	224(	-60)
		280(	-64)	140(	-68)	112(	-72)	126(	-76)	140(	-80)	252(	-84)	224(	-88)	98(	-92)

				96(	-96)	112(	-100)	133(	-104)	196(	-108)	140(	-112)	126(	-116)	224(	-120)	140(	-124)
				112(	-128)	84(	-132)	112(	-136)	84(	-140)	196(	-144)	238(	-148)	84(	-152)	140(	-156)
				112(	-160)	84(	-164)	140(	-168)	112(	-172)	84(	-176)	140(	-180)	189(	-184)	56(	-188)
				168(	-192)	84(	-196)	84(	-200)	140(	-204)	56(	-208)	56(	-212)	56(	-216)	140(	-220)
				84(	-224)	112(	-228)	56(	-232)	28(	-236)	56(	-240)	56(	-244)	28(	-248)	14(	-252)

DEGREE 15

3	3	82561	256)	163841	0)	8128(	-256)						
5	3	82561	256)	163841	0)	8128(	-256)						
9	3	20801	512)	28672(	0)	2016(	-512)						
11	5	3801	512)	68001	256)	18472(	0)	6800(	-256)	316(	-512)		
13	3	82561	256)	163841	0)	8128(	-256)						
17	3	82561	256)	163841	0)	8128(	-256)						
33	3	528(	1024)	31744(	0)	496(-1024)							
43	5	380(	512)	68001	256)	18472(	0)	6800(	-256)	316(	-512)		
57	3	20801	512)	28672(	0)	2016(	-512)						
65	3	20801	512)	28672(	0)	2016(	-512)						
113	5	3801	512)	68001	256)	18472(	0)	6800(	256)	316(	-512)		
129	3	82561	256)	163841	0)	8128(	-256)						
131	3	82561	256)	163841	0)	8128(	-256)						
171	5	33(	1024)	7920(	256)	16894(	0)	7920(	-256)	1(	-1024)		
191	5	380(	512)	68001	256)	18472(	0)	6800(	-256)	316(	-512)		
209	5	380(	512)	68001	256)	18472(	0)	6800(	-256)	316(	-512)		
241	3	82561	256)	163841	0)	8128(	-256)						
383	3	82561	256)	163841	0)	8128(	-256)						
683	5	1(	2048)	30(	1024)	7920(	256)	16897(	0)	7920(	-256)		
893	5	380(	512)	68001	256)	18472(	0)	6800(	-256)	316(	-512)		
995	5	380(	512)	68001	256)	18472(	0)	6800(	-256)	316(	-512)		
1119	5	390(	512)	67361	256)	18664(	0)	6608(	-256)	380(	-512)		
1279	5	1(	2048)	30(	1024)	7920(	256)	16897(	0)	7920(	-256)		
1371	3	82561	256)	163841	0)	8128(	-256)						

1913	5	380(	512)	6800(	256)	18472(	0)	6800(	-256)	316(	-512)								
2295	5	33(	1024)	7920(	256)	16894(	0)	7920(	-256)	1(	-1024)								
2521	5	395(	512)	6740(	256)	18562(	0)	6740(	-256)	331(	-512)								
2731	5	380(	512)	6800(	256)	18472(	0)	6800(	-256)	316(	-512)								
2981	5	380(	512)	6736(	256)	18664(	0)	6608(	-256)	380(	-512)								
3643	5	33(	1024)	7920(	256)	16894(	0)	7920(	-256)	1(	-1024)								
5783	5	380(	512)	6800(	256)	18472(	0)	6800(	-256)	316(	-512)								
5813	5	33(	1024)	7920(	256)	16894(	0)	7920(	-256)	1(	-1024)								
16383	181	30(	360)	35(	356)	120(	352)	45(	348)	30(	344)	120(	340)	60(	336)	105(	332)		
		90(	328)	90(	324)	105(	320)	165(	316)	75(	312)	90(	308)	120(	304)	90(	300)		
		90(	296)	240(	292)	90(	288)	90(	284)	375(	280)	90(	276)	120(	272)	210(	268)		
		90(	264)	90(	260)	195(	256)	195(	252)	90(	248)	270(	244)	195(	240)	90(	236)		
		375(	232)	120(	228)	105(	224)	360(	220)	120(	216)	180(	212)	135(	208)	90(	204)		
		180(	200)	165(	196)	210(	192)	120(	188)	315(	184)	150(	180)	105(	176)	360(	172)		
		135(	168)	150(	164)	420(	160)	150(	156)	165(	152)	240(	148)	105(	144)	285(	140)		
		245(	136)	210(	132)	180(	128)	213(	124)	165(	120)	90(	116)	525(	112)	120(	108)		
		150(	104)	525(	100)	155(	96)	180(	92)	315(	88)	165(	84)	180(	80)	300(	76)		
		195(	72)	135(	68)	225(	64)	225(	60)	165(	56)	510(	52)	120(	48)	195(	44)		
		270(	40)	120(	36)	150(	32)	285(	28)	180(	24)	240(	20)	420(	16)	180(	12)		
		135(	8)	225(	4)	286(	0)	120(	-4)	360(	-8)	150(	-12)	135(	-16)	345(	-20)		
		135(	-24)	300(	-28)	360(	-32)	135(	-36)	180(	-40)	300(	-44)	180(	-48)	120(	-52)		
		300(	-56)	270(	-60)	150(	-64)	555(	-68)	105(	-72)	120(	-76)	360(	-80)	150(	-84)		
		180(	-88)	210(	-92)	120(	-96)	165(	-100)	195(	-104)	225(	-108)	150(	-112)	300(	-116)		
		300(	-120)	180(	-124)	330(	-128)	135(	-132)	135(	-136)	375(	-140)	120(	-144)	180(	-148)		
		360(	-152)	90(	-156)	150(	-160)	240(	-164)	240(	-168)	120(	-172)	300(	-176)	150(	-180)		
		105(	-184)	330(	-188)	90(	-192)	150(	-196)	390(	-200)	180(	-204)	210(	-208)	195(	-212)		
		105(	-216)	165(	-220)	255(	-224)	120(	-228)	105(	-232)	255(	-236)	180(	-240)	90(	-244)		
		255(	-248)	150(	-252)	135(	-256)	250(	-260)	120(	-264)	105(	-268)	165(	-272)	90(	-276)		
		123(	-280)	180(	-284)	150(	-288)	120(	-292)	165(	-296)	105(	-300)	75(	-304)	285(	-308)		
		60(	-312)	60(	-316)	225(	-320)	45(	-324)	95(	-328)	75(	-332)	60(	-336)	90(	-340)		
		90(	-344)	60(	-348)	30(	-352)	45(	-356)	15(	-360)								

DEGREE 16

259	5	26498(	768)	128(	512)	16384(	256)	21888(	0)	24448(-256)
383	5	548(	1024)	54000(	512)	112161	256)	24420(	0)	23952(-256)
511	4	108800(	512)	256(	256)	32640(	0)	21760(	-256)	
1021	5	540(	1024)	54000(	512)	110561	256)	24540(	0)	23920(-256)
3857	4	16(	4096)	30720(	256)	4080(	0)	30720(	-256)	
7399	4	108800(	512)	256(	256)	32640(	0)	21760(	-256)	

1JC93		6	10986	10241	229161	2561	163201	01	261121	-2561									
32767	256		161	5121	481	5081	801	5041	641	5001	641	4961	641	4721	1601	4881	641	4841	
			961	4801	1281	4761	961	4721	1921	4681	1801	4641	1121	4601	1401	4561	2401	4521	
			1281	4481	1281	4441	1281	4401	1281	4361	2721	4321	1921	4281	1281	4241	2241	4201	
			1601	4161	961	4121	1921	4081	2561	4041	1281	4001	4001	3961	2081	3921	1921	3881	
			1921	3941	2881	3801	2881	3761	1281	3721	2561	3681	1921	3641	1921	3601	3041	3561	
			1921	3521	3201	3481	3121	3441	1601	3401	3521	3361	1601	3321	1281	3281	2561	3241	
			1921	3201	2081	3161	2241	3121	3201	3081	1921	3041	2561	3001	4481	2961	1921	2921	
			4001	2881	3201	2841	1281	2801	2881	2761	2561	2721	2241	2681	4801	2641	1921	2601	
			3841	2561	3841	2521	2561	2481	1921	2441	1921	2401	5281	2361	1281	2321	2561	2281	
			3041	2241	1921	2201	3841	2161	3201	2121	1921	2081	2561	2041	4801	2001	3521	1961	
			1921	1921	2241	1881	1921	1841	4001	1801	3841	1761	2241	1721	2561	1681	4481	1641	
			1921	1601	3841	1561	3361	1521	2241	1481	5761	1441	2561	1401	1921	1361	2881	1321	
			5761	1281	2881	1241	2881	1201	3201	1161	1921	1121	4321	1081	2561	1041	1921	1001	
			3521	961	2401	921	4481	881	2561	841	2561	801	2881	761	3401	721	3201	681	
			2241	641	2881	601	5441	561	1761	521	2561	481	3841	441	2561	401	6241	361	
			2561	321	2881	281	3841	241	2881	201	2561	161	3201	121	2561	81	2241	41	
			2571	01	4161	-41	2241	-81	4801	-121	5001	-161	1601	-201	4801	-241	3201	-281	
			1921	-321	4001	-361	1921	-401	3681	-441	2561	-481	5121	-521	2561	-561	1921	-601	
			4481	-641	1601	-681	5761	-721	2561	-761	2561	-801	4481	-841	3841	-881	2041	-921	
			3841	-961	4161	-1001	2561	-1041	5121	-1081	4001	-1121	1921	-1161	1921	-1201	5601	-1241	
			1601	-1281	2561	-1321	3841	-1361	1921	-1401	4801	-1441	2081	-1481	3201	-1521	2561	-1561	
			2561	-1601	3361	-1641	2561	-1681	2561	-1721	2561	-1761	3841	-1801	5121	-1841	1921	-1881	
			3841	-1921	4801	-1961	1281	-2001	2561	-2041	1921	-2081	3201	-2121	4241	-2161	3201	-2201	
			3201	-2241	1921	-2281	3201	-2321	3201	-2361	2881	-2401	2241	-2441	1601	-2481	3201	-2521	
			2561	-2561	1441	-2601	3841	-2641	4161	-2681	1921	-2721	3841	-2761	2561	-2801	1761	-2841	
			2881	-2881	2561	-2921	1921	-2961	1601	-3001	4801	-3041	1921	-3081	2241	-3121	3201	-3161	
			2241	-3201	5121	-3241	2321	-3281	2401	-3321	2241	-3361	2401	-3401	1601	-3441	1921	-3481	
			2561	-3521	1281	-3561	3201	-3601	3361	-3641	1281	-3681	1921	-3721	2561	-3761	1601	-3801	
			2561	-3841	1921	-3881	1281	-3921	2881	-3961	1281	-4001	1601	-4041	2241	-4081	3361	-4121	
			1921	-4161	1281	-4201	1921	-4241	801	-4281	2561	-4321	2241	-4361	961	-4401	2561	-4441	
			1601	-4481	961	-4521	1281	-4561	1281	-4601	1601	-4641	801	-4681	1281	-4721	641	-4761	
			961	-4801	1921	-4841	641	-4881	1281	-4921	641	-4961	481	-5001	961	-5041	161	-5081	

APPENDIX B

INVERSE PAIR RELATION OF CYCLOTOMIC COSET LEADERS

In APPENDIX B the inverse pair relation of cyclotomic coset leaders is given for $3 \leq n \leq 14$. If two cyclotomic coset leaders r and q are such that $r \cdot q \equiv 2^k \mod 2^n-1$ and $r \leq q$, then r and q are given in pair with q in parentheses.

EXAMPLE: For n = 7, two cyclotomic cosets containing 9 and 15 are inverse of each other as mentioned above. For n = 9 the cyclotomic coset containing 75 is a self-inverse since $(75)^2 = 5625 \equiv 2^2 \mod 511$.

INVERSE PAIR RELATION OF CYCLOTOMIC COSET LEADERS

DEGREE 3 2 PAIRS

1(1) 3(3)

DEGREE 4 2 PAIRS

1(1) 7(7)

DEGREE 5 4 PAIRS

1(1) 3(11) 5(7) 15(15)

DEGREE 6 4 PAIRS

1(1) 5(13) 11(23) 31(31)

DEGREE 7 10 PAIRS

1(1) 3(43) 5(27) 7(55) 9(15) 11(13) 19(47) 21(31) 23(29)
63(63)

DEGREE 8 12 PAIRS

1(1) 7(37) 11(29) 13(59) 19(47) 23(61) 31(91) 43(43) 53(53)
127(127)

DEGREE 9 26 PAIRS

1(1) 3(171) 5(103) 9(57) 11(93) 13(59) 15(239) 17(91) 19(27)
25(25) 29(93) 37(185) 39(95) 41(187) 43(107) 45(125) 47(47) 51(171)
55(223) 61(111) 75(75) 79(123) 83(117) 85(127) 109(109) 255(255)

DEGREE 10 32 PAIRS

1(	1)	5(	2951	7(	439)	13(	79)	17(	181)	19(	175)	23(	89)	25(	41)	29(	267)
35(	95)	37(	33)	43(	119)	47(	109)	49(	107)	53(	251)	59(	191)	61(	151)	71(	265)
73(	127)	85(	45)	91(	215)	101(	157)	103(	149)	115(	347)	129(	221)	147(	239)	173(	479)
179(	383)	223(	367)	235(	379)	343(	343)	511(	511)								

DEGREE 11 90 PAIRS

1(	1)	3(	683)	5(	411)	7(	293)	9(	231)	11(	139)	13(	315)	15(	137)	17(	365)
19(	493)	21(	99)	25(	87)	27(	77)	29(	75)	31(	231)	33(	63)	35(	117)	37(	83)
39(	105)	41(	693)	43(	143)	45(	91)	47(	47)	51(	201)	53(	309)	55(	135)	57(	413)
59(	249)	61(	237)	67(	153)	71(	179)	73(	85)	79(	183)	81(	149)	83(	509)	85(	151)
101(	537)	103(	153)	107(	249)	109(	695)	111(	203)	113(	471)	119(	501)	121(	423)	127(	233)
129(	479)	127(	837)	141(	369)	147(	349)	149(	735)	155(	383)	157(	339)	163(	249)	165(	211)
167(	331)	169(	393)	171(	205)	175(	503)	179(	223)	181(	475)	185(	213)	187(	427)	191(	493)
199(	995)	215(	219)	217(	217)	221(	343)	229(	295)	235(	429)	245(	667)	247(	473)	251(	367)
255(	731)	301(	959)	307(	767)	311(	311)	317(	381)	329(	379)	333(	375)	341(	511)	349(	351)
359(	727)	371(	669)	415(	439)	443(	495)	469(	703)	477(	751)	491(	763)	687(	879)	1023(	1023)

DEGREE 12 76 PAIRS

1(	1)	11(	373)	17(	261)	19(	229)	23(	893)	29(	989)	31(	661)	37(	1003)	41(	103)
43(	667)	47(	437)	53(	233)	59(	629)	61(	1007)	67(	191)	71(	757)	73(	731)	79(	473)
83(	1531)	89(	559)	97(	719)	101(	223)	107(	621)	109(	113)	121(	863)	127(	1387)	137(	751)
139(	349)	149(	859)	151(	607)	157(	313)	163(	179)	167(	859)	173(	503)	181(	141)	187(	943)
197(	317)	199(	227)	209(	1783)	211(	991)	239(	1919)	251(	311)	253(	511)	277(	281)	283(	941)
293(	547)	307(	337)	313(	347)	331(	631)	341(	853)	349(	1021)	361(	743)	367(	733)	379(	643)
397(	733)	439(	691)	481(	1013)	489(	489)	657(	657)	661(	695)	663(	667)	667(	1493)	673(	807)
691(	813)	693(	1471)	583(	1759)	819(	1013)	871(	727)	889(	1367)	701(	701)	821(	821)	827(	827)
829(	993)	877(	1699)	887(	1393)	2047(	2047)										

DEGREE 13 316 PAIRS

1(	1)	3(	2741)	5(	1633)	7(	3511)	9(	911)	11(	745)	13(	635)	15(	3823)	17(	1453)
19(	645)	21(	1911)	23(	1791)	25(	983)	27(	1517)	29(	283)	31(	2977)	33(	1263)	35(	703)
37(	665)	39(	1471)	41(	993)	43(	381)	45(	1277)	47(	177)	49(	1003)	51(	1747)	53(	1391)
55(	143)	57(	723)	59(	1411)	61(	941)	63(	4031)	65(	127)	67(	367)	69(	831)	71(	347)
73(	1911)	75(	1215)	77(	1343)	79(	985)	81(	839)	83(	691)	85(	3567)	87(	1933)	89(	1749)
91(	1533)	93(	669)	95(	97)	97(	1003)	101(	811)	103(	1511)	105(	1019)	107(	595)	109(	2029)
111(	349)	113(	351)	115(	3063)	117(	2339)	119(	413)	121(	433)	123(	333)	125(	729)	131(	2939)
133(	185)	135(	875)	137(	293)	139(	825)	141(	179)	145(	173)	147(	969)	151(	1899)	153(	589)
155(	647)	157(	1213)	159(	979)	161(	973)	163(	1759)	165(	695)	167(	1919)	169(	933)	171(	241)
175(	1651)	181(	1145)	183(	761)	187(	1193)	189(	2037)	191(	1245)	195(	2815)	197(	395)	199(	2043)
211(	2597)	233(	1871)	265(	919)	287(	277)	289(	921)	311(	1359)	313(	971)	315(	1487)	317(	441)

219(6377)	221(10011)	224(5511)	225(4055)	227(12643)	229(6651)	231(4611)	233(8791)	235(17099)	
237(19711)	239(9771)	241(3751)	245(13711)	247(12277)	249(9551)	251(3591)	253(19833)	255(11899)	
257(27511)	267(5831)	269(2751)	271(9771)	273(5111)	277(3231)	281(3791)	285(27995)	287(16911)	
291(14231)	293(6991)	295(17511)	297(29151)	301(12791)	303(9471)	305(13731)	307(6271)	309(6131)	
311(5771)	313(13987)	315(*15251)	317(17831)	319(15151)	325(12351)	327(17911)	329(14591)	331(8291)	
335(12471)	337(11911)	341(17551)	343(27471)	345(10211)	349(3991)	351(12371)	355(6231)	357(7171)	
361(27271)	365(7641)	371(19651)	374(5491)	383(6631)	391(16551)	394(18551)	397(19111)	401(13891)	
403(15451)	407(37131)	409(7411)	411(4591)	415(5731)	419(9971)	421(6911)	423(13751)	425(14071)	
427(16491)	429(13951)	431(20431)	433(9271)	435(6971)	437(11811)	439(7651)	441(8731)	443(9431)	
445(6971)	447(10431)	451(6331)	455(15831)	457(7351)	461(12031)	467(5911)	469(12751)	471(17571)	
473(13951)	475(9651)	477(17731)	479(27051)	483(16651)	487(7571)	489(20311)	493(6151)	495(11751)	
499(28071)	501(13571)	503(16611)	505(3571)	509(19171)	547(35191)	553(6471)	557(6931)	559(6011)	
563(9751)	565(6851)	567(6791)	569(13391)	571(12631)	575(7551)	585(10231)	587(6071)	591(14311)	
595(13051)	597(9811)	599(20111)	603(5691)	605(8531)	611(7391)	617(27751)	619(8871)	621(8591)	
629(37351)	631(17171)	639(15071)	651(14471)	653(7151)	655(7131)	659(19131)	661(7591)	671(13551)	
677(14671)	683(18491)	701(30031)	711(8411)	719(29991)	725(19151)	727(27431)	731(11391)	733(25451)	
741(9711)	747(13411)	749(13671)	751(9551)	767(12711)	793(14631)	795(9171)	797(9151)	799(8151)	
805(9871)	813(17431)	819(30711)	821(13271)	823(15031)	827(16591)	839(15231)	843(14451)	847(12671)	
851(15311)	855(12551)	857(14051)	861(14471)	869(14611)	875(27391)	883(20141)	895(12311)	899(12071)	
901(13331)	903(30551)	905(14371)	923(15951)	925(18511)	935(14631)	937(29111)	939(9531)	951(19811)	
959(13611)	989(19571)	991(17111)	1007(18731)	1015(12691)	1017(28111)	1171(27351)	1173(12291)	1179(39471)	
1185(17891)	1197(12391)	1205(17751)	1211(12531)	1259(29351)	1325(38391)	1331(18771)	1343(19091)	1345(20471)	
1357(15911)	1389(14931)	1393(17231)	1435(29911)	1455(27431)	1459(27791)	1491(17251)	1495(16071)	1527(17471)	
1529(13791)	1529(35511)	1653(20271)	1703(17271)	1717(19751)	1719(30071)	1771(30471)	1871(18871)	1973(35751)	
6995(6995)									

DEGREE 14 380 PAIRS

1(1)	5(32771)	7(23411)	11(15011)	13(13391)	17(28931)	19(8691)	23(7131)	25(9831)	
29(5451)	31(5291)	35(6491)	37(4431)	41(12051)	47(38351)	49(3351)	53(9371)	55(23831)	
59(30551)	61(13431)	65(27731)	67(2451)	71(9231)	73(11231)	77(19151)	79(2091)	83(*37751)	
85(55011)	89(35591)	91(16211)	95(18971)	97(35471)	101(34071)	103(1691)	107(38291)	109(1551)	
113(1451)	115(4631)	119(15231)	121(6771)	125(42631)	131(3931)	133(13551)	137(25151)	139(5731)	
143(34371)	149(53551)	151(2171)	157(17871)	161(9191)	163(33171)	167(18471)	173(9471)	175(40271)	
179(17391)	181(24971)	185(19111)	187(2631)	191(34311)	193(14131)	197(40751)	199(2471)	203(35511)	
205(2411)	211(24771)	221(27431)	223(5511)	227(3611)	229(17171)	233(24411)	235(7671)	239(6171)	
251(7191)	253(16191)	265(4331)	269(12791)	271(6851)	275(10131)	277(29391)	281(16911)	283(71351)	
287(35791)	293(25511)	295(7271)	299(15891)	305(10211)	307(38491)	311(7911)	313(15311)		
317(7651)	319(9791)	323(37291)	325(54951)	329(56271)	331(27671)	337(29491)	341(60071)	343(34391)	
347(35611)	349(16631)	353(17231)	355(40151)	359(12351)	367(6711)	371(19631)	373(5711)	377(24511)	
379(39351)	389(6371)	391(29751)	395(9711)	397(26931)	401(33911)	403(14231)	407(29661)	409(6011)	
413(11511)	415(7551)	419(19991)	421(13291)	425(11951)	427(37991)	431(13311)	437(19371)	439(8631)	
445(17391)	451(36511)	455(39251)	457(4751)	461(56151)	467(23511)	479(13511)	481(34891)	485(19931)	
487(29271)	491(19011)	493(13431)	497(13791)	499(8231)	503(6451)	505(19791)	509(12071)	511(76631)	
513(14311)	535(24231)	539(13071)	541(14991)	547(7691)	553(29331)	557(7391)	563(27731)	569(7811)	
575(20231)	581(36191)	583(19931)	587(33231)	589(9771)	595(15071)	599(14591)	605(9531)	607(37551)	
613(19511)	619(30671)	623(9731)	625(39671)	629(16931)	631(8571)	647(37731)	649(29031)	653(11291)	
655(35831)	659(7211)	661(11651)	667(29231)	679(9411)	683(14231)	689(26871)	691(46551)	695(37011)	
697(16411)	701(17531)	703(40791)	707(18771)	709(19671)	715(9911)	725(25091)	727(17211)	743(39471)	
745(11711)	751(37351)	757(23591)	761(11411)	763(24231)	785(15071)	787(18951)	793(9711)	797(17891)	
799(9411)	803(17751)	805(14451)	809(20051)	811(34551)	815(9851)	821(13371)	823(27471)	827(14471)	
839(15611)	845(19971)	847(35591)	851(19451)	859(15071)	875(27941)	877(14391)	881(11391)	883(37671)	
887(19731)	893(24771)	895(55511)	905(11451)	907(14271)	911(13971)	913(35351)	917(17491)	925(25931)	
931(12671)	935(35471)	943(13031)	949(14331)	953(14291)	955(13211)	959(39591)	965(18851)	967(70311)	
999(14691)	937(33071)	1003(38391)	1007(35631)	1009(29391)	1015(24051)	1019(30071)	1093(54711)	1099(14251)	

1103(5315)	1109(5983)	1111(2411)	1115(2485)	1117(4093)	1127(1381)	1133(1991)	1135(3421)	1147(2671)	
1163(1651)	1175(1715)	1177(3967)	1181(1519)	1183(1759)	1187(2719)	1189(1399)	1193(13871)	1199(3293)	
1211(1437)	1214(3959)	1223(3791)	1225(1445)	1229(1491)	1231(3361)	1237(4013)	1241(1703)	1243(1865)	
1253(3965)	1255(1325)	1259(3071)	1261(3287)	1271(1405)	1273(6139)	1277(2015)	1301(5503)	1315(1657)	
1319(1975)	1327(1943)	1357(5813)	1367(3901)	1369(2549)	1373(2995)	1375(4087)	1379(1941)	1385(5879)	
1391(2815)	1403(1333)	1421(1741)	1435(7159)	1447(2027)	1459(1471)	1463(2363)	1465(1711)	1469(3803)	
1475(5819)	1513(1765)	1517(2735)	1525(2675)	1529(1705)	1535(2497)	1595(2949)	1609(1933)	1615(2039)	
1627(2769)	1639(3511)	1655(1913)	1679(6079)	1685(5999)	1687(2197)	1709(2347)	1727(2647)	1735(2389)	
1747(2473)	1751(2911)	1757(1781)	1771(2903)	1783(3023)	1831(5467)	1835(2491)	1847(3823)	1853(3037)	
1855(2941)	1871(3445)	1901(2663)	1907(3465)	1929(2669)	1939(3733)	1949(2099)	1957(6107)		
1973(2453)	2003(2475)	2011(3707)	2029(2405)	2035(5557)	2045(3517)	2047(5451)	2347(3581)	2357(3319)	
2371(2533)	2395(2525)	2419(3515)	2431(2555)	2453(6071)	2455(2983)	2459(2445)	2471(3325)	2479(4091)	
2483(5643)	2507(3575)	2519(2543)	2527(7151)	2557(3415)	2677(5563)	2711(3499)	2717(3895)	2731(2731)	
2741(8063)	2765(5623)	2771(5590)	2783(3797)	2791(4021)	2797(5887)	2861(7679)	2867(6143)	2909(3503)	
2935(3031)	2971(4031)	2993(5611)	3005(3931)	3295(3565)	3383(3821)	3413(3413)	3709(7039)	3757(6127)	
4761(4011)	8191(8191)								

DEGREE 15 904 PAIRS

1(1)	3(10923)	5(6555)	9(3641)	11(2979)	13(2523)	15(2185)	17(1935)	19(1725)	
23(1425)	25(1311)	27(1517)	29(1131)	33(993)	37(1107)	39(861)	41(999)	43(765)	
45(731)	47(3573)	51(645)	53(2473)	55(633)	57(575)	59(2777)	61(3223)	65(3529)	
67(1471)	69(675)	71(3231)	73(4041)	75(437)	77(3733)	81(2857)	83(1977)	85(387)	
87(377)	89(12151)	95(345)	97(5743)	99(931)	101(2271)	103(995)	107(919)	109(977)	
111(369)	113(1451)	115(285)	117(7019)	121(11031)	123(933)	125(1847)	127(16255)	129(255)	
131(4815)	135(5583)	137(725)	139(3065)	141(1191)	143(691)	145(685)	149(1103)	153(215)	
157(1441)	159(2247)	163(7039)	165(211)	167(1375)	169(1745)	171(5557)	173(2463)	177(1491)	
179(921)	181(5431)	183(1971)	185(1949)	187(7535)	191(193)	195(7899)	197(499)	199(6093)	
201(8151)	205(4953)	207(7519)	209(7939)	213(1077)	219(1467)	221(8157)	223(2351)	225(2747)	
227(1011)	229(4723)	233(2391)	235(1817)	237(3181)	239(5077)	241(3471)	243(1753)	247(4925)	
249(659)	251(4751)	253(3607)	261(1381)	263(4859)	265(981)	267(5033)	269(3249)	271(18031)	
275(835)	277(2011)	281(1341)	283(3821)	289(2381)	291(6647)	293(671)	295(2333)	297(1879)	
303(2359)	305(757)	309(967)	307(937)	309(5037)	311(11695)	313(969)	317(3831)	319(2003)	
321(1945)	323(3551)	325(3743)	327(703)	335(2841)	337(681)	339(3673)	347(12431)	349(845)	
351(6531)	353(5241)	355(5815)	359(639)	361(3903)	363(3701)	365(1975)	367(2411)	373(2899)	
375(6903)	379(2335)	381(9181)	383(4791)	389(3959)	391(4947)	393(1605)	395(1081)	397(423)	
401(5685)	405(1881)	407(3945)	409(3685)	411(2791)	415(3711)	417(1493)	419(1369)	421(1947)	
425(6853)	429(3819)	431(2965)	433(1527)	437(3691)	439(2911)	443(7919)	445(3019)	447(843)	
449(321)	451(5885)	457(6009)	459(4783)	461(2631)	463(2947)	467(1809)	471(447)	473(3257)	
477(5839)	479(1947)	481(3383)	485(1423)	489(8175)	491(2269)	493(997)	495(7043)	501(4055)	
503(3563)	505(5701)	507(719)	509(8063)	521(4717)	523(1549)	529(3039)	533(1429)	535(7869)	
545(1179)	549(547)	563(3319)	565(5351)	569(657)	551(2477)	555(2903)	557(5471)	559(7523)	
561(3417)	563(8113)	585(2733)	589(7095)	571(1779)	573(5547)	579(5493)	583(7775)	585(2433)	
587(3633)	591(11255)	593(1713)	597(2311)	599(5619)	601(2617)	603(2717)	605(2329)	607(3293)	
611(1377)	617(635)	615(1455)	617(4949)	619(1641)	621(4063)	625(8024)	627(2451)	629(6095)	
631(4095)	633(3251)	643(5065)	647(3191)	649(1263)	653(1957)	655(963)	661(5109)	663(2719)	
667(1523)	669(3853)	673(5307)	675(3835)	677(1791)	683(5805)	687(14971)	689(2901)	697(2045)	
699(7971)	701(795)	703(5595)	711(6063)	715(7659)	717(3519)	723(4855)	727(2299)	729(7599)	
731(5599)	737(2223)	739(3969)	741(2211)	743(3495)	745(3357)	747(1623)	751(6763)	753(7093)	
759(1511)	761(2971)	767(3375)	779(4515)	781(2811)	783(1721)	785(2707)	787(2873)	789(2035)	
793(4757)	799(11775)	801(2659)	803(857)	807(6613)	809(4911)	811(2595)	813(4771)	815(4709)	
817(2073)	823(1785)	825(6831)	827(4719)	829(5599)	831(7551)	839(7689)	849(3949)	851(3273)	
853(6129)	855(10999)	859(8125)	863(1215)	865(1591)	867(2231)	869(2451)	871(1831)	873(4917)	
877(1343)	879(2667)	881(5455)	885(2925)	887(5435)	891(3935)	893(3229)	895(8027)	901(1273)	
905(2935)	907(11067)	909(3429)	911(1695)	913(8111)	915(6361)	923(4047)	925(5287)	927(1479)	

REFERENCES

1. Zierler, N., "Linear Recurring Sequences," Journal of the Society for Industrial and Applied Mathematics, Vol. 7, No. 1, March, 1959, pp. 31-48

2. Gold, R., "Study of Correlation Properties of Binary Sequences," Aeronautical Systems Division, Wright-Patterson AFB, Ohio, Report No. R-692, January, 1964, AD-431113

3. Gold, R., "Characteristic Linear Sequences and Their Coset Functions," Journal of the Society for Industrial and Applied Mathematics, Vol. 14, No. 5, September, 1966, pp. 980-985

4. Gold, R., "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE Transactions on Information Theory, Vol. IT-13, No. 4, October, 1967, pp. 619-621

5. Gold, R., "Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions," IEEE Transactions on Information Theory, Vol. IT-14, No. 1, January, 1968, pp. 154-156

6. Kasami, T., "Weight Distribution Formula for Some Class of Cyclic Codes," Report of Coordinated Science Lab., University of Illinois, Urbana, Illinois, R-285, 1966, AD-632574

7. Kasami, T., Lin, S. and Peterson, W. W., "Some Results on Cyclic Codes which Are Invariant under the Affine Group and Their Applications," Information and Control, Vol. 11, 1968, pp. 475-496

8. Kasami, T., "Weight Distributions of Bose-Chaudhuri-Hocquenghem Codes," chapter 20 in R. C. Bose and T. A. Dowling(eds.), Combinatorial Mathematics and Its Applications, The University of North Carolina Press, Chapel Hill, North Carolina, 1969

9. Solomon, G., "Tri-Weight Cyclic Codes," Jet Propulsion Lab., Pasadena, California, Space Programs Summary, 37-41, Vol. IV

10. Golomb, S. W., Shift Register Sequences, Holden-Days, Inc., San Francisco, California, 1967

11. Golomb, S. W., "Theory of Transformation Groups of Polynomials Over GF(2) with Applications to Linear Shift Register Sequences," Information Sciences, Vol. 1, No. 1, December, 1968, pp. 87-109

12. Welch, L. R., "Cross-Correlation and Quadratic Forms," Department of Electrical Engineering, University of Southern California, Los Angeles, California, unpublished notes

13. Trachtenberg, H. M., "On the Cross-Correlation Functions of Maximal Linear Recurring Sequences," Ph.D. Dissertation, Department of Electrical Engineering, University of Southern California, Los Angeles, California, January, 1970

14. Mattson, H. F. and Solomon, G., "A New Treatment of Bose-Chaudhuri Codes," Journal of the Society for Industrial and Applied Mathematics, Vol. 9, No. 4, December, 1961, pp. 654-669

15. Peterson, W. W., Error Correcting Codes, The M.I.T. Press and John Wiley & Sons, Inc., New York, 1961

16. Dowling, T. A. and McEliece, R., "Cross-Correlations of Reverse Maximal-Length Shift Register Sequences," Jet Propulsion Lab., Pasadena, California, Space Programs Summary, 37-53, Vol. III, pp. 192-193

17. Carlitz, L. and Uchiyama, S., "Bounds for Exponential Sums," Duke Mathematical Journal, Vol. 24, 1957, pp. 37-41

18. Pless, V., "Power Moment Identities on Weight Distributions in Error Correcting Codes," Information and Control, Vol. 6, 1963, pp. 147-152

19. McEliece, R. J., "Efficient Solutions of Equations for Decoding," Jet Propulsion Lab., Pasadena, California, Space Programs Summary, 37-40, Vol. IV, pp. 216-218

20. Dickson, L. E., Linear Groups with an Exposition of the Galois Field Theory, Dover Publications, Inc., New York, 1958

21. Berlekamp, E. R., Algebraic Coding Theory, McGraw-Hill, Inc., New York, 1968

22. Kasami, T., "Weight Enumerators for Several Classes of Subcodes of the 2nd Order Binary Reed-Muller Codes," Information and Control, Vol. 18, 1971, pp. 369-394